НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Інформаційно-комунікаційні технології»
спеціальності 172 «Телекомунікації та радіотехніка»
на тему: «Аналіз процедур забезпечення якості у мобільних мережах 5G»

Виконав:
студент IV курсу, групи ТІ-61
Волосянко Кирило Сергійович _____

Керівник:
професор кафедри ІТМ ІТС, д.т.н., с.н.с.
Скулиш Марія Анатоліївна _____

Рецензент:
доцент кафедри ТК ІТС, к.т.н., доцент,
Міночкін Дмитро Анатолійович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ
на дипломну роботу студенту
Волосянко Кирилу Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи: «**Аналіз процедур забезпечення якості у мобільних мережах 5G**» керівник роботи професор кафедри інформаційно-телекомунікаційних мереж Скулиш Марія Анатоліївна, д.т.н., с.н.с., затверджені наказом по університету від від «30» березня 2020 р. №924-с

2. Термін подання студентом роботи 09.06.2020 р.

3. Вихідні дані до роботи: 1.Спеціальна література 2.Матеріали мережі інтернет. 3 Власні спостереження/знанння. 4. Матеріали з пудручників.

4. Зміст роботи (перелік завдань, які потрібно розробити):

1) Ознайомлення з 5G
2) Опис наданих сервісів
3) Вимоги до якості
4) Опис механізмів LTE
5) Протоколи гарантії якості в мережах доступу і на рівні ядра мережі

6) Процедура гарантування якості обслуговування

5. Дата видачі завдання 01.10.2019 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Визначення та затвердження теми	20.01.2020	виконано
2	Визначений план роботи	24.01.2020	виконано
3	Ознайомлення з 5G	05.02.2020	виконано
4	Виконання першого розділу	06.03.2020	виконано
5	Ознайомлення з механізмами LTE та виконання другого розділу	21.04.2020	виконано
6	Ознайомлення з процедурами гарантування якості	13.05.2020	виконано
7	Завершення роботи, її оформлення	07.06.2020	виконано

Студент Кирило ВОЛОСЯНКО

Керівник роботи Марія СКУЛИШ

РЕФЕРАТ

Робота містить 74 сторінок, 24 малюнки та 4 таблиці. Було використано 7 джерел.

Мета роботи: підвищення якості надання послуг кінцевим користувачам мобільних мережах 5G за рахунок поєднання доступних засобів керування.

В даній роботі розглядається технологія 5G, принцип роботи, вимоги до якості мережі. Також ознаюмлюємось з технологією SDN, її архітектурою та принципами роботи.

Проведено аналіз технології SDN та 5G, описані недоліки SDN, також переваги 5G та вимоги до її якості.

Ключові слова: SDN, 5G, програмно – конфігуровані мережі, надійність, резервування, перемаршрутизація, показники надійності.

ABSTRACT

The work contains 74 pages, 24 drawings and 4 people. 7 sources were used.

Purpose: to improve the quality of services to end users of 5G mobile networks through a combination of available controls.

In any case, you can use 5G technology, working, requiring other users to follow. We will also define with SDN technology, its architecture and principles of work. Analytical technologies of SDN and 5G are carried out, shortcomings of SDN, and also 5G are described and necessary for its work.

Key words: SDN, software - configured networks, reliability, redundancy, re - routing, reliability indicators.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AMPS	Advanced Mobile Phone Service (аналоговий стандарт стільникового зв'язку, що відноситься до мереж (1G))
API	Application programming interface (набір готових функцій, що надаються додатком)
CDMA	Code Division Multiple Access(технологія зв'язку, при якій канали передачі мають загальну смугу частот)
GSM	Groupe Spécial Mobile (глобальний стандарт цифрового мобільного стільникового зв'язку)
GSA	GlobalMobileSuppliersAssociation(Глобальна асоціація постачальників мобільного обладнання)
HSPA	High Speed Packet Access (технологія бездротового широкосмугового радіозв'язку, яка використовує пакетну передачу даних)
IoT	Internet of Things (концепція обчислювальної мережі фізичних предметів, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем)
IMT	International Mobile Telecommunication system (Міжнародна система мобільних телекомунікацій)
LTE	Long-Term Evolution (стандарт бездротової високошвидкісної передачі даних для мобільних телефонів і інших терміналів, що працюють з даними)
NFV	Network Functions Virtualization (це концепція мережевої архітектури, що пропонує використовувати технології віртуалізації для віртуалізації цілих класів функцій мережевих вузлів у вигляді складових елементів)
OFDM	Orthogonal frequency-division multiplexing (цифрова схема

	модуляції, яка використовує велику кількість близько розташованих ортогональних піднесучих)
QoS	quality of service (ймовірність того, що мережа зв'язку відповідає заданій угоді про трафік)

ВСТУП

Актуальність теми: В умовах сучасного світу дослідження технологій та мереж бездротового зв’язку являється надзвичайно важливим завданням, оскільки використання якісного та високошвидкісного зв’язку є важливим пріоритетом більшості розвинених держав. Провідні технологічні держави світу поставили за мету впровадити 5G до 2020 року. Цій технології визначена роль локомотива розвитку телекомунікаційна також лідера технологічного розвитку і технологій цифрової трансформації. Технологія 5G стане вирішальною інновацією, яка забезпечить високошвидкісним та більш надійним мобільним зв’язком, здатну справлятися з постійно зростаючими вимогами до передачі даних як з боку бізнесу, так і рядових користувачів. 5G надасть величезні можливості для підвищення продуктивності і зросання цифрової економіки. Наявність необхідних частот є одним з основних чинників для розвитку таких мереж, поряд з готовністю мережевої архітектури та інфраструктури, бізнес-моделей і абонентських пристроїв.

Мета роботи: підвищення якості надання послуг кінцевим користувачам мобільних мережах 5G за рахунок поєднання доступних засобів керування.

Завдання поставлені в роботі: Ознайомитись з технологією 5G, SDN, принципами роботи технологій та механізмів, описати вимоги до якості, механізми LTE.

Об'єкт дослідження: процес забезпечення якості кінцевим користувачам мобільних мереж 5g.

Предмет дослідження: технологічні рішення для мереж 5-го покоління.

Наукова новизна: проведено аналіз сучасних рішень, виявлено переваги та недоліки розгортання мережі 5-го покоління та особливості забезпечення якості обслуговування.

Практична цінність: Розроблено рекомендації щодо розгортання мереж 5-го покоління та організації гібридного телекомунікаційно-

обчислювального середовища для забезпечення якості обслуговування кінцевих користувачів.

РОЗДІЛ 1.

ТЕХНОЛОГІЇ 5G

1.1 Ознайомлення з технологією 5g

За основу для технології 5g було взято мережі NGN

Згідно з визначенням, наведеним в Рекомендації MCE-T Y.2001, мережа наступного покоління (NGN) - це мережа з пакетною комутацією, здатна забезпечити користувачів різноманітними вузькосмуговими і широкосмуговими послугами, включаючи послуги телефонного зв'язку. Вона заснована на широкосмуговій мережі з пакетною технологією транспортування, що забезпечує необхідну якість послуг QoS, в якій функції, пов'язані з наданням послуг, не залежать від технологій транспортування інформації. Мережа NGN дає користувачам необмежений доступ до різноманітних послуг провайдерів і підтримує узагальнену мобільність, яка дозволяє користувачам отримати доступ до послуг у будь-якому місці і в будь-який час.

У рекомендації MCE-T Y.2012 перераховані основні принципи функціональної архітектури NGN:

Підтримка багатьох технологій доступу - функціональна архітектура NGN вимагає гнучкої конфігурації, необхідної для підтримки груп технологій доступу.

Розподілене керування - використання принципу розподіленої обробки в пакетних мережах і підтримка прозорості розташування для розподілених обчислень.

Відкрите керування - мережеві інтерфейси керування мають бути відкритими для підтримки процесів створення нових, зміни існуючих послуг та підтримки засобів забезпечення логіки послуг сторонніх постачальників.

Незалежність надання послуг - процес надання послуг має бути розділений між функціями транспортної мережі, яка працює з використанням механізму розподіленого відкритого керування. Це підтримує конкурентне

оточення під час розвитку NGN, сприяє прискоренню процесів впровадження нових послуг.

Для реалізації цих функцій в Рекомендації ITU-T Y.2011 [i] запропоновано базову еталонну модель NGN, яка включає два рівні: рівень послуг NGN (service stratum) і рівень транспорту NGN (transport stratum), кожен з яких містить по три площини: користувача, керування та менеджменту (Рис. 1.1).

Рис. 1.1 Базова еталонна модель NGN (із рекомендації MCE-T Y.2011)

Функціональність рівнів базової еталонної моделі NGN наведено на Рис. 1.2 (рекомендації ITU-T Y.2012). На кожному з рівнів використовують декілька функцій, так для надання послуг (прикладних сервісів кінцевим користувачам) застосовують функції підтримки прикладних сервісів і послуг, відповідні керуючі функції. NGN підтримує точку сполучення з функціональною групою прикладних сервісів, так званий інтерфейс прикладних сервісів мережі (application network interface-ANI), який реалізує канал взаємодії та обміну інформацією між прикладними сервісами і елементами мережі NGN. ANI забезпечує ресурси, необхідні для реалізації прикладних сервісів. Транспортний рівень забезпечує послуги IP-з'єднань для користувачів мережі NGN за допомогою функцій керування транспортом, включаючи функції керування мережевими підключеннями NACFs (Network

Attachment Control Functions) і функції керування ресурсами та доступом RACFs.

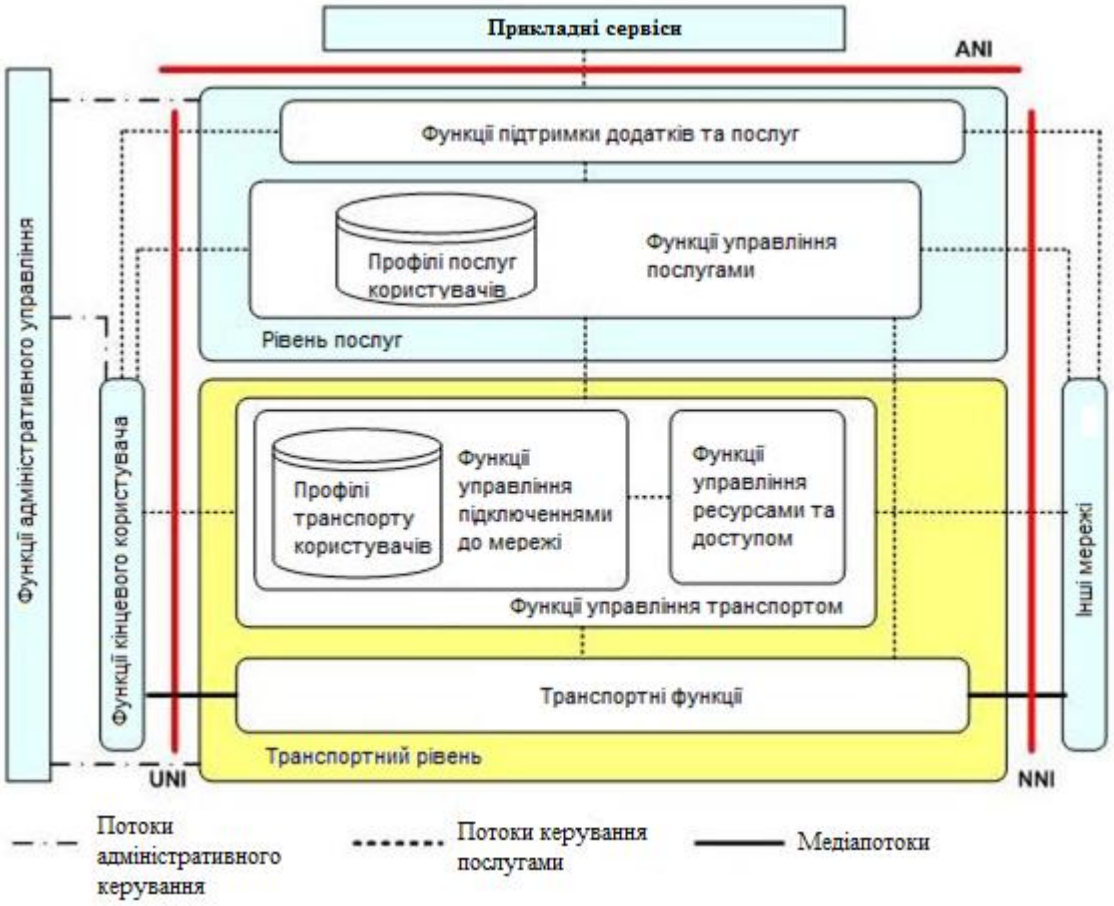


Рис. 1.2 Загальна функціональна архітектура NGN

Відповідно до Рекомендації MCE-T Y.2011 функції транспортного рівня включають безпосередньо транспортні функції і функції керування транспортом.

Транспортні функції (transport functions) забезпечують з'єднання всіх компонент і фізично розділених функцій всередині NGN. Ці функції підтримують передачу медіаінформації, а також інформації керування (сигналізації) та технічного обслуговування. Транспортні функції включають функції мережі доступу, прикордонні функції, функції транспортного ядра (магістралі) і функції шлюзів.

Функції мережі доступу (access network functions) забезпечують підключення кінцевих користувачів до мережі, а також збір і агрегацію трафіку, що надходить з мережі доступу в транспортну магістраль (ядро). Ці

функції також реалізують механізми керування якістю обслуговування QoS, пов'язані безпосередньо з трафіком користувача, включаючи керування буферами, чергами і розкладами, пакетну фільтрацію, класифікацію трафіку, маркування трафіку, визначення політик обслуговування і формування профілю передачі трафіку.

Функції мережі доступу залежать від використовуваної технології доступу, наприклад, вони відрізняються для бездротової технології CDMA та провідної технології доступу xDSL. Залежно від технології, яка використовується для доступу до послуг NGN, мережа доступу включає функції, пов'язані з:

- кабельним доступом;
- доступом за технологіями xDSL;
- бездротовим доступом (наприклад, технології IEEE 802.11 (WiFi), 802.16 (WiMAX), доступ 3G RAN);
- оптичним доступом.

Прикордонні функції (edge functions) використовують для обробки трафіку, який виходить шляхом агрегування трафіку, що надходить з різних мереж доступу і передається в магістральну транспортну мережу. Вони включають функції, пов'язані з підтримкою якості обслуговування QoS і керування трафіком. Прикордонні функції використовують також між магістральними транспортними мережами.

Магістральні транспортні функції (core transport functions) відповідають за гарантовану передачу інформації через транспортну мережу з різним рівнем якості. Вони забезпечують механізми реалізації заданого рівня якості передачі QoS для користувача трафіку включаючи керування буферами, чергами і розкладом, фільтрацію пакетів, класифікацію, маркування і формування трафіку, контроль дотримання правил обслуговування, керування шлюзами і функції міжмережевих екранів.

Функції шлюзів (gateway functions) забезпечують можливості взаємодії з функціями кінцевих користувачів і/або іншими мережами, включаючи інші

типи мереж NGN та ряд існуючих мереж, таких як ТфЗК/ISDN, публічний Інтернет та інші. Функції шлюзів можуть керуватися або безпосередньо функціями рівня керування або через функції керування транспортною мережею.

Функції обробки медіаінформації (media handling functions) забезпечують обробку медіаінформації при наданні послуг, таких як генерація тональних сигналів і перекодування. Ці функції реалізують спеціальними ресурсами обробки медіаінформації на транспортному рівні.

Функції керування транспортною мережею (transport control functions) включають функції керування ресурсами та доступом, функції керування приєднанням до мережі.

Функції керування ресурсами та доступом RACFs діють як арбітр між функціями керування послугами і транспортними функціями для підтримки QoS і пов'язані з керуванням транспортними ресурсами в мережі доступу і в магістральній транспортній мережі. Рішення з керування ґрунтується на інформації про необхідий транспорт, угодах про заданий рівень обслуговування SLA, правилах мережевої політики, пріоритетах послуг та інформації про стан і використання транспортних ресурсів. Функції RACF забезпечують абстрактний підхід до інфраструктури транспортної мережі для функцій керування послугами SCFs і надають сервіс-провайдерам можливість не залежати від мережевої топології, зв'язності, завантаження ресурсів, механізмів/технологій QoS та ін. Функції RACF взаємодіють з функціями SCF і транспортними функціями для різних прикладних програмних компонентів (наприклад, SIP-виклики, потокове відео й ін.), що вимагає керування транспортними ресурсами NGN, включаючи керування QoS, керування NAPT/Firewall і проходження трансляції мережевих адрес на рівні портів NAPT.

Функції керування підключенням до мережі NACFs забезпечують реєстрацію на рівні доступу та ініціалізацію функцій кінцевого користувача для послуг доступу NGN. Ці функції забезпечують транспортний рівень

ідентифікацією/авторизацією, керуючи простором IP-адрес в мережі доступу і аутентифікації сесій доступу. Вони також повідомляють кінцевим користувачам про контактні точки до функцій NGN на рівні послуг. Функції NACF включають транспортний профіль користувача, який зберігатися у вигляді функціональної бази даних, що включає інформацію користувача, а також інші дані керування.

Рівень послуг (service stratum) включає:

- Функції керування послугами, включаючи функції профілів послуг користувачів;
- Функції підтримки прикладних програмних компонентів і функції підтримки послуг.
- Функції кінцевих користувачів.
- Функції адміністративного керування

Функції керування послугами (service control functions) включають керування ресурсами, функції реєстрації, аутентифікації та авторизації для різних сервісів на рівні послуг. Вони також можуть включати функції керування медіаресурсами, такими як спеціалізовані пристрої та шлюзи на сигнальному рівні. Функції керування послугами підтримують профілі послуг користувачів, які є комбінацію інформації користувача та інших даних керування, індивідуальний профіль кожного користувача, такі дані зберігають у функціональних базах даних.

Функції підтримки прикладних програмних компонентів і функції підтримки послуг (application support functions and service support functions) включають функції шлюзів, реєстрації, аутентифікації та авторизації на рівні прикладних програмних компонентів. Ці функції доступні в функціональних групах «прикладні сервіси» і «кінцеві користувачі». Вони працюють спільно з функціями керування послугами для забезпечення кінцевих користувачів і прикладних сервісів необхідними послугами NGN. Через інтерфейс «користувач-мережа» UNI функції підтримки прикладних програмних компонентів і функції підтримки послуг забезпечують точку доступу до

функцій кінцевих користувачів. Взаємодія прикладних програмних компонентів з даними функціями здійснюється через точку доступу, реалізовану інтерфейсом «прикладна програма-мережа» ANI.

Функції кінцевих користувачів (end-user functions) не визначають ніяких обмежень на інтерфейси користувача і мережі доступу кінцевих користувачів, які можуть бути з'єднані з мережею доступу NGN. Термінальні пристрої користувачів послуг NGN є будь-якими мобільними або стаціонарними пристроями.

Функції адміністративного керування (management functions) забезпечують можливість керувати мережею NGN для надання послуг із заданим рівнем якості, безпеки та надійності. Ці функції розподіляються децентралізовано по всім функціональним блокам (FE) і вони взаємодіють з функціональними блоками керування мережевими елементами, керування мережею і керування послугами. Функції адміністративного керування використовують на транспортному рівні і рівні послуг і для кожного з рівнів вони реалізують такі завдання:

- Керування процесом усунення відмов (Fault Management);
- Керування конфігурацією мережі (Configuration Management);
- Керування розрахунками з користувачами і постачальниками послуг (Accounting Management);
- Контроль продуктивності мережі (Performance Management);
- Забезпечення безпеки роботи мережі (Security Management).

З метою більш простого розуміння принципів побудови мереж наступного покоління в більшості публікацій з NGN наводиться узагальнена 4-х рівнева архітектура NGN, в якій виділяються такі рівні (Рис. 1.2):

Рис. 1.2 Чотирьохшарова модель NGN

- рівень доступу, який містить мережу абонентського доступу до транспортної пакетної мережі;
- транспортний рівень, який включає магістральну пакетну мережу (мережу, побудовану на базі протоколів пакетної комутації IP або ATM, на сьогоднішній день найчастіше на базі технології MPLS та протоколу IP);
- рівень керування комутацією, включає сукупність функцій з керування усіма процесами обслуговування викликами в телекомунікаційній мережі;
- рівень послуг та експлуатаційного керування, який містить логіку виконання послуг та/або прикладних програмних компонентів, керує цими послугами, має відкриті інтерфейси для використання сторонніми організаціями (для розробки нових сервісів).

Термінальне обладнання рівня доступу не входить до складу мережі NGN. Безпосереднє підключення до мережі можливо тільки для пакетних абонентських терміналів, які працюють з використанням протоколів SIP та H.323.

Концепція NGN спричинила еволюцію систем керування в телекомунікаціях від спеціальних апаратних рішень до програмно-керованих

мереж (SDN), які здійснюють контроль та керування відповідним обладнанням гетерогенних інформаційно-телекомунікаційних систем.

1.1.1 SDN

Система мережевої інфраструктури, що використовується в даний час, підтримується майже в тому ж вигляді протягом десятиліть, в той час як технології продовжують розвиватися. Управління ресурсами має найважливіше значення в мережевих сценаріях, давнє і досі відкрите питання. Більше того, у цьому сценарії головне питання для вирішення яким є роз'єднання логіки управління мережею від площини даних мережі, тобто фізичні маршрутизатори та комутатори, які передають трафік від джерела до пунктів призначення. Оскільки існує багато мережевих парадигм які намагаються знайти ефективну альтернативу класичній архітектурі Інтернету, лише деякі з них широко поширені та успішні. У цьому конкурсі парадигма програмно-визначених мереж (SDN) є однією з найкращих і найбільш привабливими рішеннями для вдосконалення Інтернету з більшою гнучкістю та проблеми адаптивності. Ця нова мережева парадигма дозволяє централізуватись програмно для управління поведінкою всієї мережі шляхом відокремлення площини рішення маршрутизації від рівня переадресації. Парадигмі SDN потрібен механізм для здійснення зв'язку між керуванням і даними можливої площини. Ця функціональність отримується за допомогою нового протоколу OpenFlow. SDN спільно з OpenFlow дозволяє нам писати програми управління високого рівня, які задають поведінку мережевих компонентів. Ці програми можуть піклуватися про різні мережеві завдання, наприклад, безпеку, маршрутизацію та управління ресурсами. Ці завдання є одними з найважливіших аспектів у всіх мережевих сценаріях, оскільки основні Інтернет-сервіси, як правило, все ще базуються на класичній парадигмі BestEffort.

З одного боку, послуга Best-Effort проста, простота була найважливішим фактором, який визначив її світовий успіх. З іншого боку, на

жаль, сервіс Best-Effort не може забезпечити будь-яку гарантію пропускної здатності, затримки в кінці та втрати пакету. Крім того, нині попит на якість, пов'язаний з транспортуванням даних ЗМІ зростає, як в наукових колах, так і в промисловості. Ця потреба являє собою дуже важкий виклик, і це вимагає значних зусиль для забезпечення якості, що підтримується QoS мережею.

Традиційно QoS визначається з точки зору доступності, тобто у відсотках часу, в який система відліку працює. Таким чином угоди про рівень обслуговування (SLAs) були визначені як функція відсотка доступності, наприклад, 99,999%, відомий як "п'ять дев'яток", що передбачає час простою 5,26 хвилин на рік. Простій - це час, необхідний для ідентифікації та усунення несправності у з'єднанні чи на обладнанні. Крім того, це дуже важливо розуміти, що кожен тип послуг має різні вимоги SLA, а не лише на основі доступності. Отже, вдосконалена угода про домовленість повинна прийняти / враховувати затримку пакету та параметри втрати пакету на додаток до доступністі. Звідси випливає, що якість деяких типів додатків залежить від затримки та / або втрати пакету (наприклад, програми в режимі реального часу або мультимедійні передачі). З одного боку, послуги телефонії (наприклад, VoIP) мають сувору затримку вимоги до пакету та кодеку. У цих програмах, якщо пакет досягає призначення після заданого порогу затримки послуга стає марною. Для додатків в режимі реального часу також непридатні для повторної передачі втрачених пакетів. З іншого боку, у нас є інші типи застосувань, які називаються еластичними.

Гарантувати вимоги щодо якості в традиційному режимі Best-Effort непросто. З цього приводу працює спеціальна група Internet Engineering (IETF) За останні десятиліття запропоновано різні архітектури QoS, такі як IntServ та DiffServ. Однак ці пропозиції не були дуже успішними або реалізовані в широкому масштабі, оскільки вони вимагають певних кардинальних змін з веб-дизайну. У сучасній архітектурі Інтернету також існує суворий характер, брак інформації про доступні мережеві ресурси від кінця до кінця точки зору. Часткове рішення надійшло від методів

мультипротокольної мітки (MPLS) та методу протоколу кордону шлюзу (BGP) [15], які є визначені для вирішення цих проблем. На жаль, цим рішенням не вистачає конфігурації та адаптивності в режимі реального часу. У цьому сценарії парадигма SDN може бути фундаментальним ключем для подолання існуючих пояснень обмежень найкращих зусиль вище.

Ця теза використовує поняття OpenFlow у SDN для управління диференціацією мережеві послуги з високим QoS. Зокрема, ми розглядаємо відеопотоки сервіс та послуга передачі даних. По-перше, ми визначаємо QoS Management і Оркестраційна архітектура, яка дозволяє нам керувати мережею в модульній формі шлях. По-друге, ми забезпечуємо чітку інтеграцію між архітектурою та стандартна парадигма SDN після розділення між контролем і площини даних. Потім ми надаємо формулу лінійного програмування (ІЛП) цілої лінійки проблема гарантування хорошого QoS з точки зору втрати та затримки пакетів, прийнято враховувати обмеження мережі, тобто максимально прийнятний пакет втрати та затримки для кожного типу послуги та наявної пропускної здатності на посиланнях. Зокрема, наша модель визначає найменший товарний потік проблеми "Path" (MCFCSP) і використовує обидві відомі проблеми, отримані в результаті дослідження операцій: проблема багатотоварного потоку (MFP) та обмежений найкоротший шлях (CSP). З огляду на оптимальне рішення проблеми, ми інтегруємо результати за допомогою емульованої мережі за допомогою мінінет. Таким чином, можна відобразити різні мережеві потоки в реальній мережі, на основі оптимального рішення з моделі. Більше того, ми визначаємо різні рівні QoS, відповідно до системи MOS для служб, які ми розглядаємо. Нарешті, ми знайшли зв’язок між оптимальним рішенням забезпечення моделлю та рівнями MOS. Ми використали ці результати для надання свідчень про ефективність нашої моделі порівняно з традиційним рішенням, яке дає емулятор.

Тоді, змінюючи мережеві умови, легко знайти нові оптимальні маршрути між джерелом та пунктом призначення за допомогою модель.

Можливо також динамічне відображення маршрутів у мережі та, найголовніше - гарантувати необхідність забезпечення якості. Ця робота є першим кроком на шляху розгортання нашої пропозиції у Університеті Каліфорнії, Лос-Анджелес (UCLA), мережа містечка з диференційованими послугами та суворими вимогами щодо якості.

Масштабованість

Традиційні локальні мережі не дуже масштабуються, підтримуючи рух схід-захід оскільки щонайменше один пристрій рівня 3 і, швидше за все, декілька пристроїв 3 рівня, знаходяться на шляху від кінця до кінця. SDN дозволяє IT-організаціям перейти до масштабної моделі мереж, за допомогою якої вони додають мережеву функціональність при необхідності, а контролер SDN дозволяє їм керувати всіма функціональними можливостями мережі, як якщо б це був один пристрій. Ключовим фактором щодо масштабованості SDN є кількість комутаторів, які може підтримувати контролер SDC. У сучасних умовах IT-організації повинні сподіватися, що придбані ними контролери можуть підтримувати як мінімум 100 комутаторів, але вони також повинні розуміти, що кількість комутаторів, які може підтримувати контролер, буде залежати від випадків використання SDN, які підтримуються.

IT-організації, які оцінюють SDN, повинні усвідомлювати той факт, що мережеві трансляції накладних витрат обмежать масштабованість рішень, які вони реалізують. Як результат, оцінюючи SDN-контролери, IT-організаціям слід переконатися, що контролер може пом'якшити вплив накладних передач мережі. Іншим фактором, що обмежує масштабованість SDN, є поширення записів таблиці потоків, яке відбувається, оскільки без певної форми оптимізації необхідний запис ход-за-ходом для кожного потоку. Як результат, оцінюючи SDN-контролери, IT-організаціям також необхідно переконатися, що контролер може мінімізувати розповсюдження записів таблиці потоків. Один із способів цього можна досягти, якщо контролер SDN використовує перезаписи заголовка в ядрі мережі. Якщо ця методика

реалізована, єдиний унікальний запис таблиці даних знаходиться при вході та виході в мережу.

Інший аспект масштабованості - це здатність контролера SDN створювати SDN, який може охоплювати кілька сайтів. Ця можливість дозволяє переміщувати ВМ та віртуальне сховище між сайтами. Для отримання максимальної користі від цієї можливості контролер SDN повинен дозволяти мережевій політиці маршрутизації та переадресації автоматично застосовуватись до перенесених серверів та / або сховищ.

Продуктивність

Як було описано раніше, однією з ключових функцій контролера SDN є: встановлення потоків.

Таким чином, два ключові показники ефективності, пов'язані з контролер SDN - це час настройки потоку та кількість потоків в секунду що контролер може налаштувати. Ці показники продуктивності сильно впливають на розгортання додаткових контролерів SDN. Наприклад, якщо комутатори у виробничому SDN ініціюють більше потоків, ніж це може бути підтримано існуючими контролерами SDN, потрібно додати більше контролерів.

Потоки можна налаштувати одним із двох способів: проактивно або реактивно. Настроювання активного потоку відбувається до того, як пакет надійде до комутатора OpenFlow, і тому коли перший пакет надходить на перемикач OpenFlow, комутатор вже знає, що робити з пакетом. Це призводить до незначної затримки настройки та відсутності реального обмеження кількості потоків в секунду, яке може підтримувати контролер. В ідеалі контролер SDN попередньо заповнює таблиці потоків максимально можливим ступенем.

Навпаки, налаштування реактивного потоку відбувається, коли перемикач OpenFlow отримує пакет, який не відповідає записам таблиці даних, і, отже, комутатор повинен відправити пакет на контролер для обробки. Після того як контролер вирішує, як обробляти потік, що

інформація кешується за допомогою перемикача OpenFlow контролер SDN визначає, як довго зберігати кеш-пам'ять живою. Час, пов'язаний з налаштуванням реактивного потоку, - це сума часу, необхідного для передачі пакета від перемикача OpenFlow до контролера SDN; час обробки в контролері SDN та час, необхідний для відправлення повідомлення про зміну потоку назад до перемикача OpenFlow та заповнення таблиці потоків на комутаторі. Основні фактори, що впливають на час настройки потоку, включають потужність обробки перемикачів, які приєднані до контролера, обробку та продуктивність контролера вводу / виводу. На обробку та продуктивності контролера впливає ряд факторів. Наприклад, контролер, програмне забезпечення якого написано на C, буде швидше, ніж той, чиє програмне забезпечення написано на Java. У сучасних умовах IT-організації повинні очікувати, що контролери SDN не повинні бути вузьким місцем у створенні / видаленні записів потоку, керованих комутатором.

Мережа

У традиційному IT-середовищі конфігурація мережі здійснюється на основі пристрою. Такий підхід трудомісткий і схильний до помилок, і це призводить до невідповідностей. Цей підхід також є статичним, як і конфігурації не змінюються, оскільки змінюються умови мережі. Статичний характер традиційний підхід до програмованості мережі призводить до зниження потенційної продуктивності мережі. Як зазначалося, однією з ключових характеристик SDN є те, що в контролер є програмні інтерфейси. Одним із прикладів типу програмованості, який слід шукати IT-організаціям у контролері SDN, є можливість перенаправлення трафіку. Наприклад, з міркувань безпеки IT-організація може вибрати, щоб трафік, який входить до сервера, проходив через брандмауер. Однак, щоб не споживати ресурси брандмауера з чистим трафіком, IT-організація може захотіти вибрати перенаправлення трафіку, який виходить з сервера, щоб не проходити через брандмауер. Це складно здійснити в традиційних мережевих умовах.

Інший приклад типу програмованості, який IT-організації повинні шукати в контролері SDN, - це можливість застосувати складних фільтрів до пакетів. Ці фільтри можна вважати динамічними, інтелектуальними ACL. Прості ACL можуть базуватися на прямій відповідності заголовків пакетів і можуть бути використані для визначення, чи потрібно скидати або передавати пакети. На відміну від цього, контролер SDN повинен мати можливість застосовувати фільтри, що складаються із складних комбінацій декількох полів заголовків пакетів. Фільтри повинні мати можливість динамічно розгортатися у віртуальних мережах, і роль контролера SDN полягає в тому, щоб відсунути пов'язані записи таблиці потоків до комутаторів. Контролер SDN також може підтримувати програмованість, надаючи шаблони, що дозволяють створювати CLI-коди, що проглядаються, які, на відміну від традиційного управління конфігурацією, дозволяють динамічно програмувати мережу.

Інший спосіб, за допомогою якого контролер SDN дозволяє програмуватись, - це реалізувати API на північному рівні, як показано на малюнку 1. Інформація про управління, яка є централізованою в контролері, доступна для потенційно необмеженого набору програм SDN, які здатні динамічно змінюватися базова мережа для виконання таких завдань, як переадресація пакетів по найменш дорогому шляху або зміна параметрів QoS на основі наявної пропускної здатності або інших факторів. Ці програми SDN включають традиційні мережеві послуги, такі як брандмауер та балансири навантаження, а також системи оркестрації, такі як OpenStack. Ці додатки можуть також включати інженерію трафіку або програми, які збирають дані, які використовуються для виконання завдань, таких як управління мережею або включення чутливих до зворотного зв’язку використання.

Частина цінності, яку надає контролер SDN, - це інтелект в контролер виконує перевірку дизайну в рамках налаштування мережі і що перевірка дизайну усуває помилки вручну і, отже, збільшує мережу організації, які оцінюють контролери SDN, повинні розуміти функціональність, яку

пропонує контролер, що підвищує надійність мережі. Один з методів, який контролер SDN може використовувати для підвищення надійності мережі, вже обговорювався. Ця техніка - це можливість виявити декілька шляхів від початку походження до місця призначення. Якщо контролер SDN потім встановлює декілька шляхів між початком і пунктом призначення, на наявність рішення не впливає відключення єдиного зв'язку. Альтернативно, якщо контролер SDN встановлює лише один шлях від початку походження до місця призначення, коли стикається з відмовою посилання, контролер повинен мати можливість швидко перенаправляти трафік на активну лінію. Це вимагає, щоб контролер постійно моніторив топологію мережі.

Що стосується наявності зовнішніх з'єднань, важливо, щоб контролер підтримував технологію та альтернативи дизайну, такі як протокол надмірності віртуальної маршрутизатора (VRRP) та група агрегації з декількома шасі (MC-LAG), які призначені для підвищення надійності мережі.

Що стосується наявності самого контролера, важливо, щоб контролер був побудований з використанням як апаратних, так і програмних функцій надмірності. Також важливо, щоб контролер SDN включав кластеризацію. Наприклад, кластеризація двох контролерів SDN в режимі активного / гарячого режиму очікування підвищує надійність і кластеризацію трьох або більше контролерів SDN, при цьому один знаходиться в гарячому режимі очікування, збільшує доступність, масштабованість та продуктивність контролера SDN. Однак для того, щоб кластеризація забезпечила дуже швидкий час відмови, важливо, щоб рішення було здатне підтримувати синхронізацію пам'яті між активними та резервними контролерами.

Щоб забезпечити безпеку в мережі, контролер SDN повинен мати можливість підтримувати автентифікацію корпоративного класу та авторизацію адміністраторів мережі. Крім того, адміністратори мережі повинні мати можливість блокувати доступ до трафіку управління SDN,

дотримуючись того ж типу процедур, які вони використовують для блокування інших ключових форм трафіку, таких як трафік управління.

Деякі додаткові функції, пов'язані з безпекою, які повинен надавати контролер SDN, вже обговорювалися. Одним із прикладів такої функціональності є можливість застосувати складні фільтри до пакетів, що можна альтернативно називати здатністю реалізовувати динамічні, інтелектуальні ACL. Іншим прикладом такої функціональності є здатність контролера забезпечити, щоб кожен орендар, який обмінюється інфраструктурою, мав повну ізоляцію від усіх інших орендарів. Крім того, оскільки контролер SDN є кандидатом на зловмисну атаку, контролерам SDN потрібна можливість як обмежувати швидкість комунікацій управління, так і бути в змозі попередити мережевих адміністраторів, коли в мережі спостерігається підозра на атаку.

1.1.2 SDN Архітектура

Архітектура SDN може бути представлена трьома різними логічними шарами, як показано на Рис. 1.4.

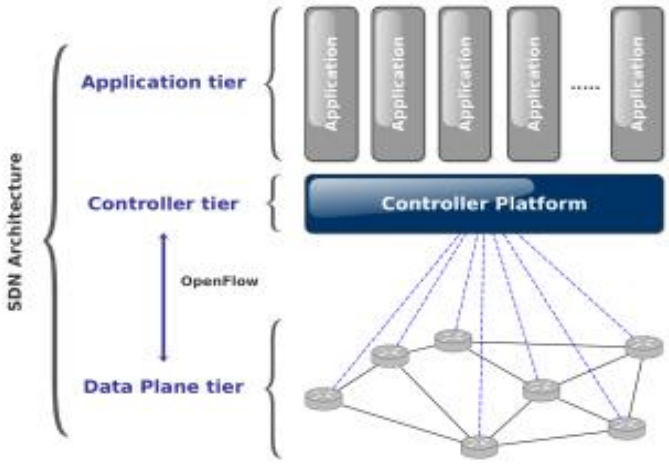


Рис.1.4 Архітектура SDN

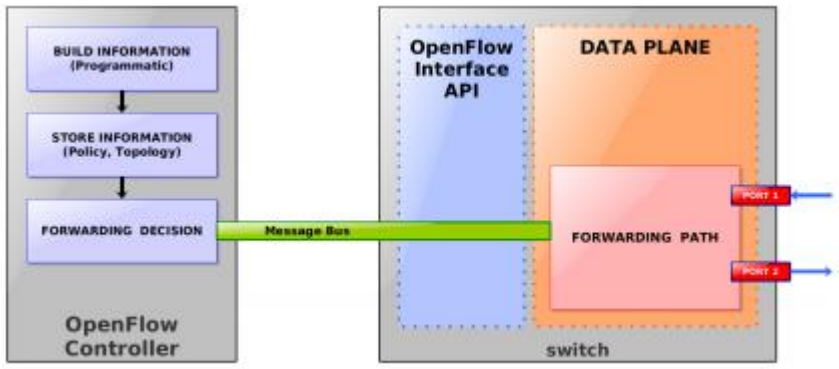


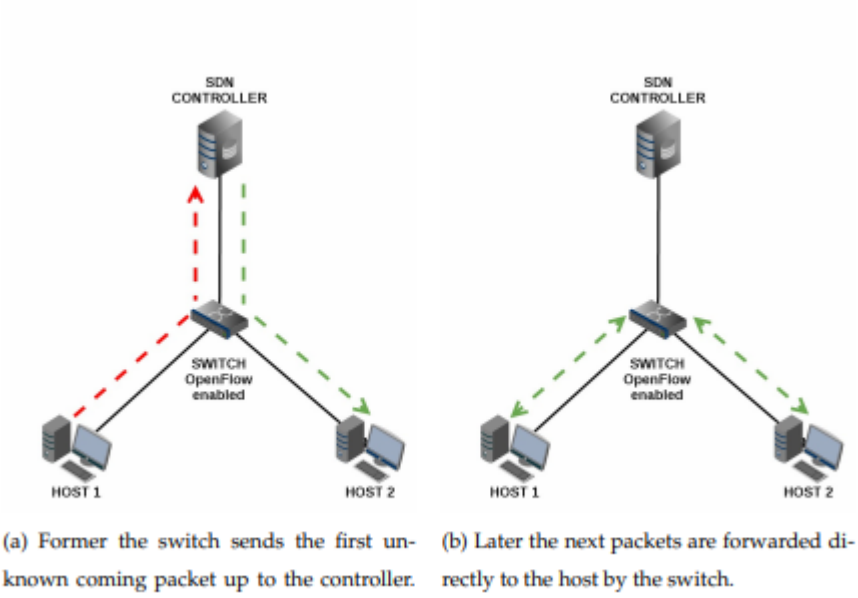
Рис. 1.5 Компоненти комутаторів SDN

SDN, відокремлюючи площину управління від площини даних, може запропонувати гнучку рамку автоматизації та управління мережею. Ця рамка робить розробку інструментів для автоматизації завдань (які виконуються вручну сьогодні) можливою. Ці засоби автоматизації можуть зменшити експлуатаційні накладні витрати нестабільність мережі, введена помилкою оператора. На жаль, програмні середовища постачальників, як правило, є власними та закритими, а їх відсутність полегшує управління та налаштування мережі. Однак SDN архітектура може полегшити інновації та забезпечити простий програмний контроль мережевого тракту даних, що породжує ідею програмованих мереж. Це важливий аспект, який дозволяє знизити бар’єр до входу для нові ідеї.

1.1.3 Принцип роботи

Коли OpenFlow Switch отримує пакет, якого він ніколи не бачив і для якого він не відповідає записів потоку, він надсилає цей пакет, який називається пакетним входом до контролера. Потім контролер приймає рішення про те, як обробляти цей пакет. Це може опустити пакет або додати запис потоку, що прямує до комутатора. У разі течії введення запису, перемикач дізнається, як передавати подібні пакети в майбутньому, як показано на Рис. 1.6. Хоча додаткові деталі цих взаємодій далі описані нижче, на даний момент цікавим є з'ясування паралелізму між описаними кроками вище та взаємодія з кешем центрального процесора (CPU). Зокрема,

коли виникає помилка кешу, дії, які зазвичай здійснює процесор, порівнянні з взаємодіями протоколу OpenFlow у разі невідповідності потоку записи. Насправді, коли ЦП потребує конкретних даних, першим кроком є пошук його в кеш (починаючи з найближчого, наприклад, кеша шару L1), як фаза пошуку в комутаторі. Якщо дані є в кеш-пам'яті, виникає звернення кешу і процесор може продовжувати наступну інструкцію. В іншому випадку процесор має для кешування пропустіть отримання даних десь в іншому місці.



(a) Former the switch sends the first unknown coming packet up to the controller.

(b) Later the next packets are forwarded directly to the host by the switch.

Рис. 1.6 Обробка пакетів за допомогою перемикачів, включених OpenFlow

Цей підхід схожий на кроки, зроблені в комутаторі, якщо не відповідає рівномірний потік записів. Подальше цікаве порівняння можна зробити між протоколом OpenFlow та функціональними можливостями (тобто, Інструкційним набором) ЦП.

Набір інструкцій

Функції, пропоновані протоколом OpenFlow, можуть бути прирівнянідо Архітектура набору інструкцій (ISA) процесора, як показано на Рис. 1.7.Починаючи з набір інструкцій дозволяє отримати доступ до внутрішньої архітектури процесора (пам'яті, протокол OpenFlow надає

зовнішньому програмному застосуванню примітиви, які можуть бути використані для програмування площини переадресації мережеві пристрої. Основні дії, які може здійснити протокол, засновані на потоках даних встановлення всередині вимикачів, як пояснено нижче.

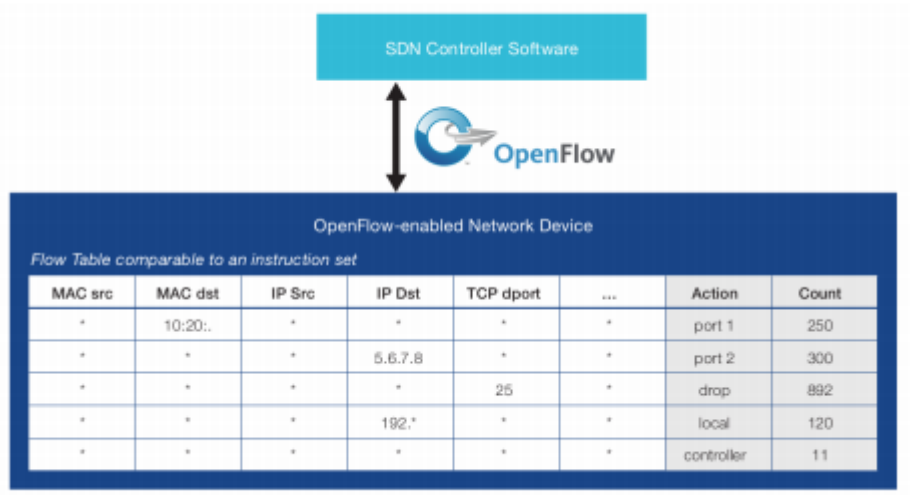


Рис. 1.7 Набір інструкцій OpenFlow

Операція на основі потоків

Протокол OpenFlow широко використовує концепцію «потоків» для ідентифікації мережевого трафіку на основі заздалегідь визначених правил узгодження, які можуть статично або динамічно запрограмовані програмним забезпеченням SDN управління. OpenFlow не тільки дозволяє мережеве програмування на основі потоку, але й забезпечує детальний контроль над потоками даних, що дозволяє мережі динамічно адаптувати ресурси за потребою. Однак це управління потоком, як правило, неможливо поточні схеми маршрутизації на основі IP. Насправді в цьому випадку все протікає між дві кінцеві точки повинні йти тим самим шляхом через мережу, незалежно відрізні їх вимоги. Перш ніж глибоко ознайомитися з останніми специфікаціями OpenFlow, подивившись на підсумок еволюції протоколу може дати нам уявлення про вдосконалення.

Підсумок еволюції

Перший випуск протоколу OpenFlow, версія 1.0, був задуманий у грудні 2009 р. Тоді, пройшовши еволюцію проміжного протоколу, OpenFlow дійшов до останньої та стабільної версії 1.4, узагальненої у Рис. 1.8.

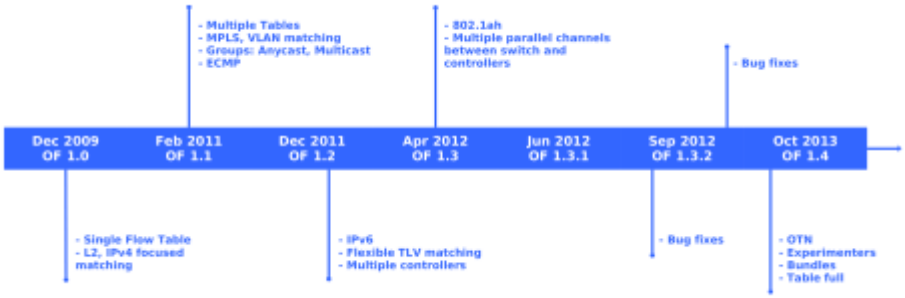


Рис. 1.8 Підсумок еволюції OpenFlow

Зокрема, основні функції першої версії OpenFlow 1.0:

1. Єдина логічна таблиця для виконання правил потоку. Більше того, цей аспект обмежує повне використання апаратних можливостей ASIC.

2. Групи для створення групових портів, аналогічні агрегації зв'язків у застарілі мережі. Це підходить для багатопоточності або надмірності.

3. Віртуальна локальна мережа (VLAN), яка підходить для грубої підтримки тегів.

4. Віртуальні порти, що розширюють OpenFlow за межами фізичних портів OpenFlow використовуватиметься для впровадження віртуалізації мережі для багатосторонніх масштабів.

5. Управління перериванням з'єднання, корисне у випадку з'єднання втрати.

Як правило, коли підключення контролера виходить з ладу або припиняється, і не вдається підключитися до резервного контролера, перемикач переходить у «аварійний стан режим "та негайно скидає поточне з'єднання TCP. У такому стані процес узгодження диктується записами таблиці аварійних потоків (позначені бітом аварійних ситуацій), тоді як будь-які інші записи видаляються. Перемикач продовжує працювати в режимі OpenFlow, поки не відновиться до контролера. Однак в останній специфікації

OpenFlow 1.4.0 було вбудовано кілька нових функцій [4]. Найважливіші удосконалення протоколу:

1. Удосконалення формату типу довжини-значення (TLV) для підвищення розширюваності протоколу. Структура TLV підходить для підтримки додаткових майбутніх експериментів.

2. Підтримка мультиконтролера робить можливою примусову взаємодію та синхронізацію між контролерами. Зокрема, моніторинг потоку дозволяє контролеру ідентифікувати в комутаторі зміни, внесені іншими контролерами. Крім того, коли оновлюється таблиця групової таблиці або лічильник таблиці, контролери, пов'язані з цим пристроєм, отримують сповіщення.

3. Атомне виконання пучка інструкцій, щоб уникнути проміжних держав. Зокрема, контролер не повинен отримувати будь-яке повідомлення, що виникає внаслідок часткового застосування пакету (збій не вдається).

4. Дрібнозерниста здатність правила допомагати контролеру керувати обмеженням можливостей для зберігання правил. Зокрема, у випадку, якщо таблиця повна, комутатори можуть проактивно вимикати правила відповідно до важливості записів. Якщо таблиці правил заповнюються, можуть бути і деякі "події вакансії" використовуються як система раннього виявлення для попередження контролера.

5. Підтримка оптичного порту дозволяє нам працювати з волоконно-оптичними мережами, керуючи частотою та потужністю, що беруть участь в оптичному зв’язку.

Наступний розділ поглиблює основні характеристики протоколу відповідно до специфікації OpenFlow 1.4.0.

Перемикання компонентів

Перемикач OpenFlow є основоположною частиною SDN. Кожен комутатор, який представлений як базове обладнання для переадресації, доступне через відкритий інтерфейс, має два різновиди:

1. "чисті" перемикачі OpenFlow не мають застарілих функцій або бортового управління, і повністю покладаються на контролер для переадресації рішень.

2. "Гібридні" комутатори підтримують OpenFlow на додаток до традиційних операції та протоколи, що робить можливою зворотну сумісність (більшість комерційні комутатори, доступні сьогодні, - це гібриди). Крім того, кожен перемикач складається із внутрішніх компонентів із трьох різних компонентів. Як показано на Рис. 1.9, основними частинами вимикача є такі:

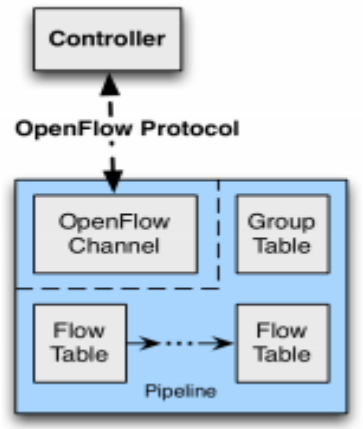


Рис. 1.9 компоненти перемикача OpenFlow

1. OpenFlow канал, який дозволяє спілкуватися та керувати між зовнішнім контролером і комутатором через протокол OpenFlow.

2. Одна або кілька таблиць потоків, які зберігають записи потоку для виконання пакету пошук і переадресація.

3. Груповий стіл, особливий вид таблиці, призначений для виконання операцій, які є загальними для безлічі потоків.

Такий підхід дозволяє складно дії переадресації, такі як багатошаровість та агрегація ліній. Канал OpenFlow - це інтерфейс, який з'єднує кожен перемикач OpenFlow до контролера. За допомогою цього інтерфейсу контролер може управляти декількома перемикає надсилання та отримання повідомлень від них відповідно до протоколу OpenFlow. Канал OpenFlow також дозволяє забезпечити безпечне спілкування серед

комутаторів і контролерів, що використовують безпеку транспортного шару (TLS) криптографічний протокол (до речі, зв’язок може здійснюватися безпосередньо через TCP). Оскільки таблиці OpenFlow вважаються ядром OpenFlow, детальною аналіз потрібен. Зокрема, таблиці OpenFlow складаються з деяких основи механізмів. Як описано в наступному розділі, найбільш важливими є: відповідність пакету, яка витягує заголовок пакета і виконує пов'язані з ним дії, і обробка конвеєра, що дозволяє комутаторам переслати та обробити пакет через ланцюг таблиці.

Обробка трубопроводів

Кожен перемикач OpenFlow може містити кілька таблиць потоків, які, як правило, складаються з декількох записів потоку, як пояснено у Розділі 2.2.4. Трубопровід Механізм обробки визначає, як пакети повинні взаємодіяти з кожною таблицею потоків, як зображено на Рис. 1.10

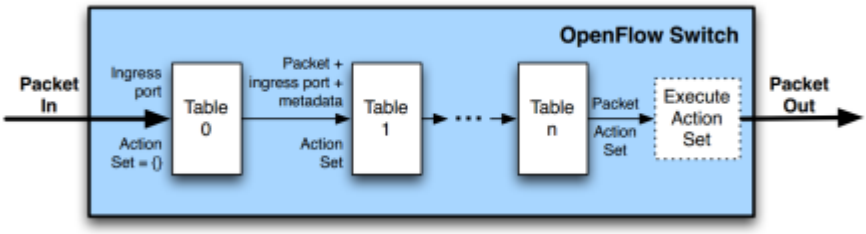


Рис.1.10 Взаємодія пакетів з таблицями потоків

Як показано на Рис. 1.10 кожен пакет узгоджується з записами потоку, починаючи з першої таблиці потоків, званої потоковою таблицею 0. Потім, залежно від За результатами попереднього матчу обробка трубопроводу може продовжуватися і тривати перейти до наступної таблиці подання для подальшої обробки. Для кожної таблиці може відбуватися відповідність пакетів, і, отже, деякі конкретні дії можуть здійснюватися комутатором. Оскільки відповідність пакетів є першою точка входу, яка консультувалася щодо процедури пошуку, більш детальна інформація щодо цього механізм необхідний.

Слабкі місця та проблеми SDN

Основна увага в цьому розділі стосується слабких сторін та проблем вирішення проблем за допомогою мереж SDN та протоколу OpenFlow. Пропозиція SDN та OpenFlow спосіб спростити прототипування, розгортання та управління мережеві елементи. Однак ми також повинні враховувати деякі цікаві аспекти, які можуть призвести мережу до небезпечного або недоступного стану наступним чином:

1. Наявність контролера - головний аспект, який необхідно зробити розглянути. Жорстка залежність між вимикачами та контролером всякий раз, коли необхідна модифікація правил, може стати проблемою. Більше того, якщо дизайн мережі враховує лише один централізований контролер, це може стати "єдиною точкою відмови". Розподілений підхід може бути реалізований для гарантування доступності та уникнення потенційний небажаний збій. Крім того, деяка надмірність або резервне копіювання розчин може бути використаний для забезпечення надійності.

2. Важлива також безпека. У SDN контролер є компонентом критичні знання мережі та цей аспект піддає контролеру до можливих атак та погроз. Крім того, канали серед контролера та комутаторів можуть бути вразливими. За даними OpenFlow специфікації, можна використовувати захищений зв'язок за допомогою протоколу TLS, але його використання залежить від дизайну мережі з його моменту, тому він не потрібен.

3. Послідовність таблиць потоків також є потенційною проблемою. З кількох контролери можуть керувати однаковими таблицями потоків, наприклад, виробництвом з цього випливає апаратний контролер та деякі інші експериментальні контролери що останній буде «найслабшою ланкою в ланцюжку». Отже, вони може бути застосовано до нижчого контролю безпеки, що веде таблиці потоків у непослідовний стан. Реалізація датчика потоку може бути придатною уникнення цих потенційних загроз.

4. Масштабованість мережі також залежить від контролера, який потенційно може стати «вузьким місцем». У випадку, якщо занадто багато

пакетів потрапить до контролер, проблеми з продуктивністю можуть виникати в мережі. З цього випливає, що важливо враховувати розподіл площини управління, для уникнення цих небажаних проблем.

5. Продуктивність мережі також може бути пов'язана з моделлю управління

прийнято. Оскільки розмір таблиці потоку обмежений, управління дуже велика кількість потоків все ще залишається сильним викликом. Однак добре розроблена мережа може знизити проблеми з продуктивністю за допомогою ініціативи підхід. Насправді, як раніше було проаналізовано у розділі 2.3.1, ініціатива підхід досягає кращих показників, ніж реактивний режим, оскільки він обмежує кількість повідомлень, що обмінюються між контролером та вимикачі. Описані вище аспекти були прийняті до уваги дослідники спільноти та представляють майбутні проблеми для SDN. В останньому розділі цієї глави представлений один з найпоширеніших контролерів, Floodlight, придатний для роботи зі SDN.

1.2 Опис сервісів які надаються

Телекомунікаційні сервіси (службові) – це послуги, які надаються у гетерогенному телекомунікаційному середовищі *в процесі організації взаємодії* між абонентами або машинами.

Сьогоднішні підприємства розгортають у своїх філіалах по декілька сервісів одночасно. Для багатьох із них підтримка виділеного автономного пристрою є надто затратною та негнучкою. В інших реалізаціях, функціональність може бути забезпечена інтегрованим маршрутизатором доступу, який може бути обмеженим у наборі функцій. По мірі того, як підприємство розвивається, все більше послуг та прикладних програмних компонентів мігрують до корпорації дата-центрів або загальнодоступних хмар, що приводить до змін в побудові корпоративних мереж. Крім того, мобільність і принцип BYOD (Bring Your Own Device – принеси свій власний

пристрій) стають все більш затребуваними, в результаті чого стають актуальними послуги запобігання витоку даних.

Зіткнувшись із необхідністю великих інвестицій, багато підприємств починають шукати альтернативні варіанти. Ці альтернативи можуть включати в себе віртуалізацію Enterprise CPE (маршрутизатора доступу) в мережу оператора.

Такі тенденції віртуалізації в поєднанні з перевагами які надає NFV забезпечують значні бізнес-можливості для постачальників послуг, які намагаються відповідати зростаючим потребам клієнтів. Традиційні IP-маршрутизатори, засновані на власному апаратному та програмному забезпеченні, є одними з найбільш капіталомістких частин інфраструктури постачальників послуг. Маршрутизатори оператора (Provider Edge routers) вичерпують ресурси платформи керування, перш ніж закінчуються ресурси платформи даних, таким чином віртуалізація функцій платформи керування покращує масштабованість.

Зберегти ресурси можна також переміщаючи функціональність маршрутизації від цільових маршрутизаторів до еквівалентних функцій, реалізованих в апаратних середовищах COTS, що забезпечують можливості хмарних обчислень, такі як NFVI.

Замість того, щоб інвестувати власний капітал у розгортання мережевої інфраструктури, постачальник послуг може надавати розширені мережеві функції. Постачальник може використовувати об’єкт VNF за допомогою інтерфейсу NFVI, який забезпечує функціональність, необхідну для впровадження клієнтського обладнання CPE та інший об’єктів VNF для платформи керування маршрутизатором оператора, покращуючи його масштабованість. Створення функціональності VNF для підприємства в якості служби можна порівняти з поняттям хмарного обчислення – «Програмне забезпечення як сервіс».

Інститут стандартизації NIST SP 800-146 [i.3] визначає програмне забезпечення як сервіс (SaaS) як можливість споживачів використовувати

прикладні програмні компоненти, що працюють у хмарній інфраструктурі. Споживач може керувати програмою лише з точки зору конфігурації та не може контролювати базову інфраструктуру.

У цьому прикладі віртуалізованих корпоративних служб VNF є прикладним програмним компонентом постачальника послуг. Підприємство є споживачем послуги. Підприємство не керує та не контролює NFVI або VNF. Підприємство як споживач VNFaaS не має інвестувати додатковий капітал у розширені мережеві функції, надані за допомогою платформи керування, а може отримати їх за певні кошти від постачальника послуг, якщо це необхідно. Постачальник послуг може масштабувати ресурси NFVI, виділені на екземпляр VNF у відповідь на збільшення використання VNF.

NIST SP 800-146 [i.3] визначили наступні переваги моделі SaaS, які також повинні застосовуватися у випадку з VNFaaS:

• Незначна роль програмного забезпечення підприємства для доступу до сервісу;

• Ефективне використання ліцензій на програмне забезпечення;

• Централізоване керування;

• Економія на попередніх витратах

Мережі постачальників послуг Pre-NFV містять пороговий маршрутизатор PE на межі ядра перед пристроєм клієнтського обладнання (CPE), як показано на Рис. 1.11. При цьому є дві бізнес-моделі; як постачальник послуг так і підприємство можуть володіти та керувати CPE.

Рис. 1.11 Постачальник послуг без віртуалізації інфраструктури підприємства

Віртуалізація інфраструктури підприємства може включати:

• Віртуалізацію функцій обладнання користувача CPE (vE-CPE) у хмарі постачальника послуг.

• Віртуалізацію функцій порогового маршрутизатора оператора PE (vPE), де функції віртуальних сервісів мережі та функцій ядра PE можуть виконуватись в хмарі постачальника послуг.

Ці два етапи є незалежними і можуть розгортатись окремо. PE маршрутизатори, як правило, надаються великій кількості клієнтів, тоді як маршрутизатор CPE використовується виключно одним клієнтом. Таким чином, економія масштабу, яку можна отримати від віртуалізації CPE є значно більшою, ніж при віртуалізації PE. Отже, віртуалізація CPE є корисною як для користувачів підприємства, так і для постачальників послуг. Віртуалізація PE може відбутись на більш пізньому етапі, щоб завершити перехід до повністю віртуалізованого рішення NFV.

У деяких архітектурах vE-CPE та vPE можуть контролюватися централізованим контролером, який виконує принципи та стандарти SDN (наприклад, OpenFlow).

Постачальник послуг несе відповідальність за розгортання, налаштування, оновлення та керування роботою екземпляру VNF для забезпечення очікуваного рівня обслуговування (SLA) для абонентів VNFaaS.

1.3 Вимоги до якості

Незважаючи на успіхи, досягнуті в області розробки мереж мобільного зв'язку четвертого покоління, з'являються нові вимоги, викликані зростаючими потребами в комунікаціях, що в свою чергу вимагає розвитку нового покоління мобільних мереж (5G). Нові можливості використання, такі як потокове відео високої роздільної здатності, віддалений моніторинг, управління в реальному часі створюють вимоги, пов'язані з пропускною здатністю, затримкою передачі, надійністю і стійкістю мережі.

Очікується, що мережі забезпечать високу безпеку, мінімальну затримку (нижче 5 мс.), надійність передачі 99,999% і стовідсоткову доступність.

Розробка мережі 5G повинна бути спрямована на подолання вищевказаних обмежень, з метою надання ультра-надійних, безпечних сервісів з мінімальною затримкою великій кількості інтелектуальних об'єктів і систем, а також новим мобільних терміналів.

Порівняння технологій 3G/4G/5G представлено на Рис.1.12 Технології IMT-2000 (3G) IMT-Advanced (4G) покращують пропускну здатність мережі, швидкість передачі даних користувачів, використання спектра і зменшують затримки. Впровадження технології IMT (5G) планується для "потужної і критично важливої машинної взаємодії", зменшення затримки, спектральної ефективності, швидкості, мобільності і надійності.

Мережева архітектура 5G складається з двох шарів: радіомережі та хмарної мережі. Різні типи базових станцій, що виконують мінімальний набір функцій, утворюють радіомережу. Хмарна мережа складається з площини користувача (User Plane Entity - UPE) і площині управління (Control Plane Entity - CPE), які виконують функції площини користувача і площини управління відповідно. Як показано на Рис. 1.13, фізична реалізація хмари може бути адаптована для задоволення різних цільових показників. Наприклад, UPE і CPE можуть бути розташовані близько до базових станцій для зменшення затримки критичних послуг. Також може бути виконано підключення БС до невеликого прилеглого центру обробки даних (ЦОД-3), а не до центрального ЦОД-2. З іншого боку, БС може бути з'єднана з ЦОД-2, якщо затримка не критична. Така гнучкість дозволяє оператору розгорнути великі і малі центри обробки даних для підтримки конкретних потреб у послугах. Така архітектура спрощує мережу і забезпечує швидке і гнучке розгортання і управління.

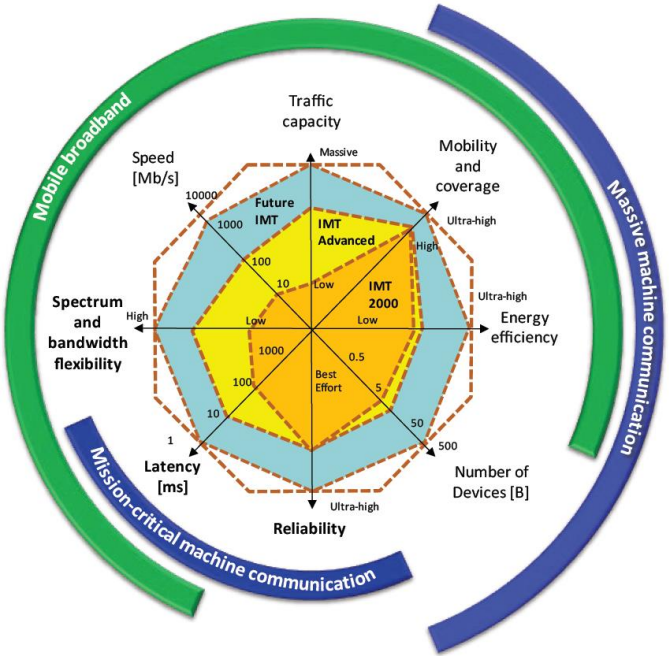


Рис. 1.12 Порівняння технологій 3G/4G/5G

Різні технології, такі як Network Functions Virtualization (NFV) і Software Defined Networking (SDN) призначені для створення і впровадження таких мереж. Проте, майбутні сервіси, такі як потокове відео та інші послуги мають різні вимоги, які підкреслюють необхідність динамічного масштабування функціональності мережі.

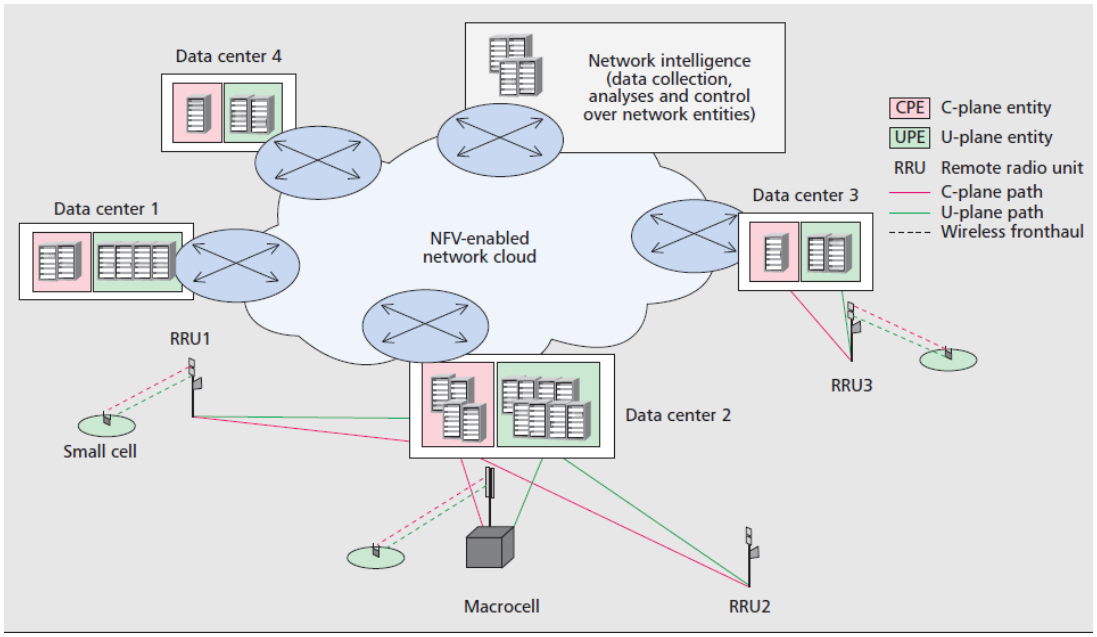


Рис. 1.13 Мережева архітектура 5G

Гетерогенні мережі відрізняються підвищеною пропускною здатністю, великим покриттям і надійністю, більш високою ефективністю використання радіочастотного спектру і низьким енергоспоживанням з боку як мережевої інфраструктури, так і термінального обладнання.

Мобільні оператори мережі стикаються з наростаючою проблемою зростання трафіку передачі даних, в зв'язку з поширеністю смартфонів і транслюванням аудіо і відео послуг. У новій парадигмі оператори повинні управляти навантаженням, задовольняючи зростаючі споживчі і корпоративні очікування продуктивності, забезпечуючи повсюдний широкосмуговий доступ, а також швидко впроваджувати нові послуги, щоб зберегти конкурентну перевагу. Існуючі мобільні мережі постійно стикаються з такими обмеженнями, як стаціонарне і дороге устаткування, складні протоколи управління і гетерогенні інтерфейси конфігурації. З метою вирішення поточних обмежень, необхідно вивчати і застосовувати принципи SDN в мобільних мережах, а саме SDMN (Software Define Mobile Networks). SDN розділяє рівні управління і передачі даних, використовуючи стандартні протоколи, що дозволяють віддаленим пристроям здійснювати управління і експлуатацію рівнів даних. Протокол синхронізації потрібен для комунікації обох рівнів, одним з таких протоколів є OpenFlow . Переваги SDN в області хмарних обчислень є очевидними, однак застосування даної концепції в мобільних мережах вимагає подальшого вивчення.

В процесі еволюції механізму управління QoS в GSM/UMTS/LTE мережах сталася міграція управління QoS з рівня користувацького обладнання до керування на рівні мережі. Цей підхід також збережеться в мережах 5G.

Механізми керування QoS в мережах 5G повинні забезпечити пріоритет відео і VoIP трафіку над іншими сервісами. Сервіс потокового відео без буферизації дуже чутливий до затримок в мережі, тому одним з найбільш важливих параметрів, який визначає вимоги до QoS є загальний час затримки

пакетів (packet delay budget - PDB). У Таблиця 1.1 наведені вимоги до затримки в 3G/4G/5G мережах.

Таблиця 1.1

Вимоги до затримки в 3G/4G/5G мережах

Терміни QoS	Запланована затримка пакетів (мс)		
	3G	4G	5G
Без гарантування якості	Не визначено	100-300	Не визначено
З гарантованою якістю	100-280	50-300	1

Ці дані показують, що з ростом покоління мобільної мережі, вимоги до нижньої межі затримки даних збільшуються. Також аналіз вимог до загальної мережевої затримки 5G показав, що вона повинна бути менше 1 мс.

На Рис. 1.14 представлено порівняння вимог до затримки на рівні управління та рівні користувача для сигнального та абонентського трафіків відповідно.

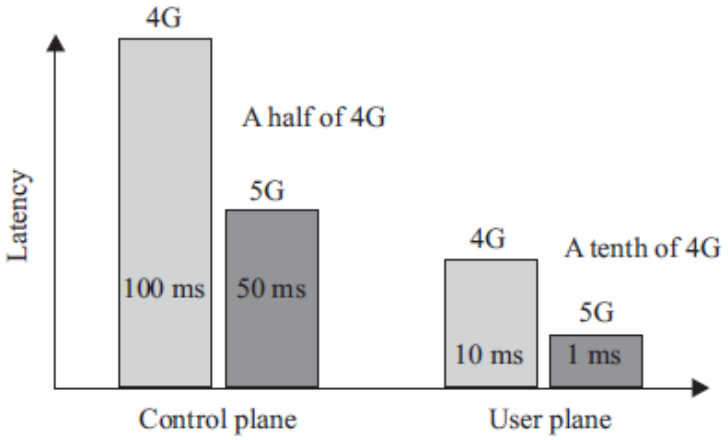


Рис. 1.14 Порівняння вимог до затримки на рівні управління та рівні користувача

На Рис 1.14 видно, що вимоги до мережі 5G будуть в два рази жорсткішими для сигнального трафіку і в 10 разів жорсткішими для абонентського трафіку.

Іншим параметром є частка втрачених пакетів через помилки при отриманні пакетів даних (IP-packet Error Rate).

Значення цього параметра, що визначає вимоги максимального числа втрат IP пакетів для широкомовного відео за допомогою мобільних мереж 3G/4G/5G, наведені в Таблиця 1.2

Таблиця 1.2

Вимоги до кількості втрачених пакетів для широкомовного відео в 3G/4G/5G мережах

Терміни QoS	Запланована затримка пакетів (мс)		
	3G	4G	5G
Без гарантування якості	10^{-2}	10^{-3}	10^{-4}
З гарантованою якістю	10^{-2}	10^{-6}	10^{-7}

Для інших сервісів якість також буде визначатися часткою втрачених пакетів в мережах 3G/4G/5G. Умови обслуговування абонентських пристроїв будуть визначатися в обох випадках: з гарантованою якістю обслуговування і без гарантованої якості. Вимоги до коефіцієнта втрат пакетів для інших послуг наведені в Таблиця 1.3.

Таблиця 1.3

Вимоги до частки втрачених пакетів для інших сервісів в 3G/4G/5G мережах

Терміни QoS	Коефіцієнт втрат пакетів (Packet Error Loss Rate)			
	SDTV	HDTV	4k UHD	8k UHD
Покоління мобільних мереж	3G/4G	4G	4G	5G
Широкомовне відео з гарантованою якістю	10^{-6}	10^{-7}	10^{-8}	10^{-9}

Розвиток концепції NFV призведе до віртуалізації функцій управління якістю, які можуть бути розділені на 2 складові: управління (Cloud QoS management function - CQMF) і контролю (Cloud QoS control function - CQCF), які показані на Рис 1.15.

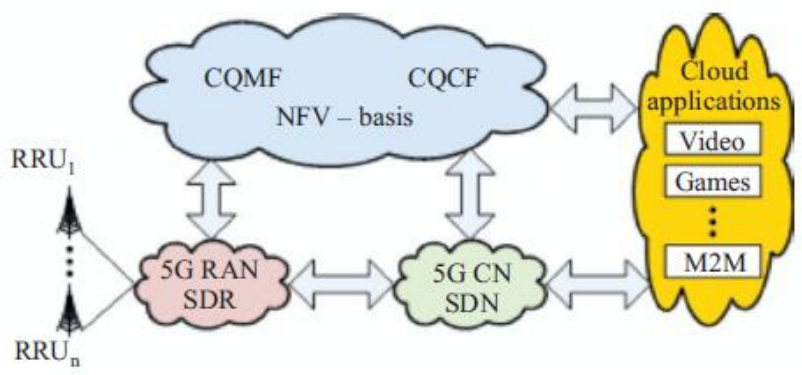


Рис. 1.15 Основні складові функцій управління якістю.

Функція CQCF забезпечує контроль потоків трафіку в режимі реального часу на основі QoS, встановленого під час з'єднання. Основні механізми управління QoS включають управління профілями трафіку, планування і управління потоками даних.

Функція CQMF забезпечує підтримку QoS в мережі 5G відповідно до SLA, а також забезпечує моніторинг, технічне обслуговування, аналіз і масштабування QoS.

Реалізація алгоритмів пріоритетності трафіку в мережах 5G буде ґрунтуватися на процедурах класифікації трафіку з акцентом на пріоритети відео-трафіку і M2M трафіку. Класифікація процедур трафіку повинна бути проведена з урахуванням можливостей адаптації: характеристики трафіку будуть динамічно змінюватися з появою нових додатків, як в M2M області, так і в області відео.

1.3.1 Показники якості послуг передачі данних

В системах мобільного зв’язку третього покоління функції контролю параметрів доступності сервісів виконувала підсистема SGSN, в ядрі EPC ці функції виконує підсистема PCRF.

На Рис. 1.16 зображена архітектура мережі передачі даних 2G/3G. Основним мережевим вузлом в цій архітектурі є вузол підтримки послуг GPRS (Serving GPRS Support Node, SGSN), який відстежує розташування абонентських терміналів передачі пакетних даних, забезпечує захисні функції і контроль доступу. SGSN з'єднується з контролером базових станцій BSC, використовуючи Frame Relay - мережу комутації фреймів (пакетів другого, канального рівня). Вузол шлюзовий підтримки GPRS (Gateway GPRS Support Node, GGSN) взаємодіє з зовнішніми мережами пакетної передачі даних (Packet Data Networks, PDNs), забезпечуючи передачу даних до/від мобільних терміналів. GGSN пов'язаний із зовнішніми мережами з пакетним перемиканням і з'єднується з вузлами SGSN через мережі, які використовують протокол IP. Керуючий блок пакетної комутації (Packet Controller Unit, PCU) забезпечує послуги пакетної радіопередачі на область охоплення BSC. Для з'єднання вузлів SGSN і GGSN з іншими елементами мережі, що забезпечують глобальну пакетну передачу даних, може додаватися кілька нових інтерфейсів (з позначенням G *, де * - символ, що визначає конкретний інтерфейс).

Розглянемо основні причини збою в роботі системи передачі даних. Однією з найбільш поширених причин є помилка, яка відправляється з боку GGSN на Gn інтерфейс. Ця помилка широко поширена в GTP повідомленнях інформаційного елемента.

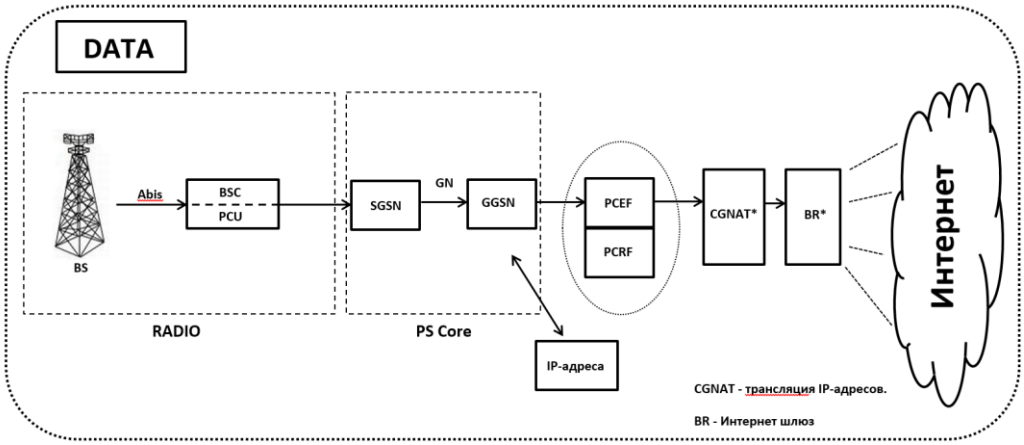


Рис. 1.16 Архітектура мережі передачі даних 2G/3G

PDP Context - набір даних про абонента, що здійснив процедуру GPRS Attach (процедуру аутентифікації і надання доступу в інтернет), який зберігається як на стороні SGSN, так і на стороні терміналу абонента, зокрема в цей набір даних входить профіль, що забезпечує певний рівень якості обслуговування абонента - QoS, призначена абоненту адреса в мережі, деякі дані про тарифікацію абонента.

Розглянемо основні показники якості сервісу передачі даних

1. Доступність

• Відсоток успішно виконаних процедур активації PDP context, ініційованих MS 2G/3G (PDP Context Activation Success Rate)

$$PDPctx\_act\_SR = \frac{PDPctx\_act\_acc}{PDPctx\_act\_req} * 100, \text{ де}$$

PDPctx_act_acc - число успішно виконаних процедур активації PDP-контексту, ініційованих MS (таймаут = 150с, після чого спроба вважається неуспішною).

PDPctx_act_req - число запитів на виконання процедури активації PDP-контексту, ініційованих MS.

• Затримка часу встановлення TCP-сесії для сервісу Web Browsing

$$WebBrowsingLatency = \frac{1}{N}\sum(WBST - WBRT)_i \text{ , де}$$

$WBST(WebBrowsingSuccessTime)$ - час встановлення TCP-сесії для сервісу Web Browsing;

$WBRT(WebBrowsingRequestTime)$ - час запиту встановлення TCP-сесії для сервісу Web Browsingi - і-ий запит встановлення TCP-сесії

N - сумарна кількість запитів за інтервал спостереження.

Відсоток блокувань в ЧНН в режимі передачі даних через перевантаження на 2G/3G (Відношення між кількістю відмов у виділенні ресурсів для передачі даних через перевантаження і загальною кількістю запитів на виділення ресурсів в ЧНН 2G/3G (Connection Block Rate).

$$ConnectionBlockRate = (PS\_BlockRate2G * Traffic2G + PS\_BlockRate3G * Traffic3G) / (Traffic2G + Traffic3G)$$

PS_BlockRate2G - відсоток блокувань в ЧНН в режимі передачі даних через перевантаженяь для мережі 2G

PS_BlockRate3G - відсоток блокувань в ЧНН в режимі передачі даних через перевантаженя для мережі 3G

$Traffic2G$ - пакетний трафік в мережі 2G в ЧНН, МВ

$Traffic3G$ - пакетний трафік в мережі 3G в ЧНН, МВ

• Відсоток успішно виконаних спроб реєстрації мобільної станції в мережі пакетної передачі даних 2G/3G (PS Attach SR).

$$PS\_Attach\_SR2G/3G = (PS\_Attach\_SR2G * Traffic2G + PS\_Attach\_SR3G * Traffic3G) / (Traffic2G + Traffic3G)$$

PS_Attach_SR2G - відсоток успішно виконаних спроб реєстрації мобільної станції в мережі пакетної передачі даних 2G;

PS_Attach_SR3G - відсоток успішно виконаних спроб реєстрації мобільної станції в мережі пакетної передачі даних 3G;

$Traffic2G$ - середньодобовий пакетний трафік в мережі 2G, МВ;

$Traffic3G$ - середньодобовий пакетний трафік в мережі 3G, МВ;

• Відсоток успішно виконаних процедур активації PDP context, ініційованих MS 2G/3G (PDP Context Activation Success Rate)

$$PDPctx\_act\_SR2G/3G = (PDPctx\_act\_SR2G * Traffic2G + PDPctx\_act\_SR3G * Traffic3G) / (Traffic2G + Traffic3G)$$

$PDPctx\_act\_SR2G$ - відсоток успішно виконаних процедур активації PDP context, ініційованих MS в 2G

$PDPctx\_act\_SR3G$ - відсоток успішно виконаних процедур активації PDP context, ініційованих MS в 3G

$Traffic2G$ - середньодобовий пакетний трафік в мережі 2G, MB

$Traffic3G$ - середньодобовий пакетний трафік в мережі 3G, MB

• Стабільність роботи центральних систем пропуску data-трафіку

$$data\_traf\_stability = 1 - \frac{t_{traf\_unstable}}{t}$$

ttraf_unstable - час нестабільної роботи систем пропуску трафіку вважається період, протягом якого рівень трафіку на PS-Core був нижче більш ніж на 20% рівня відповідного періоду минулого тижня. Показник стабільності роботи центральних систем пропуску трафіку є відношенням часу, протягом якого системи працювали стабільно, до загального часу періоду t.

2. Цілісність

• Частка успішних тестів WebBrowsing з часом закачування сторінки Kepler розміром 800 Кбайт не більше 130 секунд,

$$Activities\_WBtime < 130sec = \frac{Activities\_WBtime < 130sec}{\text{TotalActivities}} * 100\%, \text{ де}$$

$Activities\_WBtime < 130sec$ - кількість абонентських сесій з WebBrowsing Time <130sec, TotalActivities - загальна кількість абонентських сесій за період вимірювань.

• Середня швидкість передачі даних на одну абонентську активність для сервісу Web Browsing

$$WebBrowsingAverageSpeed = \frac{1}{N}\sum \text{WebBrowsingSpeed}_i, \quad \text{де}$$

i - i-а абонентська активність WebBrowsing-а

N - сумарна кількість запитів сервісу WebBrowsing.

• Частка абонентських сесій, які отримують дані при використанні VS із середньою швидкістю понад 400 кбіт/с

$$Activities\_VS > 400\text{kbps} = \frac{Activities\_VS > 400\text{kbps}}{\text{TotalActivities}} * 100\%$$, де

$Activities\_VS > 400\text{kbps}$ - кількість абонентських сесій з VideoStreaming Speed> 400kbps,

TotalActivities - загальна кількість абонентських сесій за період вимірювань.

Висновки:

Якщо подивитись на нові вимоги суспільства то стає зрозуміло, що мереж четвертого покоління вже не вистачає для деяких задач, тому їх оновлення до 5G наразі є дуже актуальнім і в деяких країнах дана технологія вже в прямому доступі.

В даному розділі пройшло ознайомлення з такими технологіями як 5G, SDN, архітектурою та принципами SDN. Були описані Вимоги до якості та сервіси які надаються (SaaS, VNFaaSta інші). Проаналізувавши технології 5G було виявлено певні недоліки, була проведена оцінка та ознайомлення з рішеннями що до їх вирішення. Розроблені рекомендації що до розгортання мереж 5-го покоління та особливостей забезпечення якості обслуговування.

РОЗДІЛ 2.

МЕХАНІЗМИ LTE, ГАРАНТІЯ ЯКОСТІ.

2.1. Опис механізмів контроля LTE

Мережа оператору мобільного зв’язку – це складна технологічна система, яка складається як з спеціалізованого телекомунікаційного обладнання.

Швидкість передачі по LTE в низхідному напрямку (до користувача) досягає 100 Мбіт/с, у висхідному - 50 Мбіт/с. Затримка на рівні користувача не перевищує 5 мс за рахунок високої ефективності використання спектра. Такі високі характеристики забезпечуються за рахунок використання декількох антен (принцип MIMO) і мультиплексування з ортогональним поділом частот OFDM на фізичному рівні.

Мережа E-UTRAN - це найперший вузол у вдосконаленій пакетній системі EPS. Вона забезпечує високу швидкість передачі даних, малу затримку на обох площинах керування і користувача, безшовне перемикання і більше покриття комірки. Розглянемо задачі, функції та процедури рівня доступу в стеку протоколів радіодоступу.

Структура E-UTRAN показана на Рис. 2.1. Мережа складається з вузлів eNodeB (eNB), які забезпечують протоколи площини користувача (PDCP/ RLC/MAC/PHY) і керування (RRC). Вузли eNB взаємодіють між собою через інтерфейс X2. Для зв'язку з удосконаленим пакетним ядром (EPC) використовується протокол S1. Обмін з вузлом керування мобільністю (MME) відбувається по інтерфейсу S1-MME, а с обслуговуючим шлюзом (SGW) - по інтерфейсу S1-U. Інтерфейс S1 підтримує зв'язки типу безліч-безліч між MME, SGW і eNB.

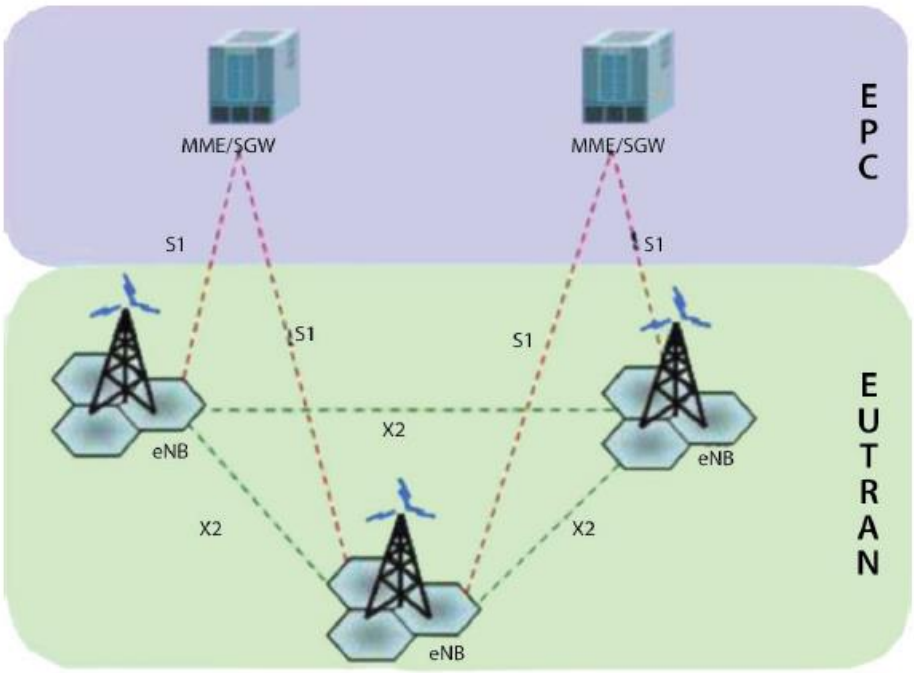


Рис. 2.1 Архітектура мережі E-UTRAN

Інформацію, яку пропускає через себе UTRAN, прийнято розділяти на два шари. До шару доступу (AS) відносяться дані, необхідні для взаємодії терміналу користувача (UE) і мережі UTRAN. Шар без доступу (NAS) містить інформацію, переноситься між базової мережею оператора (CN) і UE через UTRAN.

Рівень доступу об'єднує протоколи радіодоступу. Це протоколи, що забезпечують спільне використання радіоресурсів обладнання користувача і мережі доступу. Крім того, AS відповідає за з'єднання з каналом радіодоступу (RAB), за допомогою яких забезпечується взаємодія між UE і CN (сервіс NAS).

Рівень доступу надає обладнанню користувача можливість отримання доступу до ресурсів і сервісів мережі, а також всю необхідну інфраструктуру.

Протоколи радіодоступу виконують такі функції:

- керування ресурсами радіоканалу (RRM). Це керування радіоканалом і радіоприйомом, контроль мобільності з'єднання і динамічний розподіл ресурсів обладнання користувача в обох напрямках передачі.

- керування трафіком:

- передача даних, в т.ч. в режимі реального часу, між інфраструктурою (рівень NAS) і обладнанням користувача;
- обробка всіх типів даних при різних параметрах каналу (рівень активності, пропускна здатність, затримка передачі і ймовірність появи помилкових бітів);
- ефективне перетворення атрибутів трафіку, які використовують не-LTE прикладними програмними компонентами, в атрибути каналу радіодоступу (RAB) на рівні доступу;
- стиснення IP-заголовка і шифрування потоків даних користувача;
- самостійний вибір MME на обладнанні користувача, коли мережа не надає відповідної інформації;
- передача даних з площини користувача на SGW;
- керування розташуванням: розподіл і передача пошукових повідомлень;
- розподіл і передача широкомовної інформації;
- задання конфігурації вимірюваних параметрів і форми виведення результатів для розподілу ресурсів і забезпечення мобільності;
- розподіл і передача повідомлень про землетруси і цунамі;
- надання первинного доступу до мережі, реєстрація та приєднання до мережі або вихід з неї;
- керування передачею на різних рівнях: між eNodeB, всередині eNodeB, між eNodeB зі зміною MME, між eNodeB зі збереженням MME, але зміною SGW, між RAT;
- функціональна різноманітність і шифрування;
- кодування радіоканалу.

SAE – це архітектура ядра мережі, розроблена консорціумом 3GPP для стандарту бездротового зв'язку LTE (Рис. 2.2).

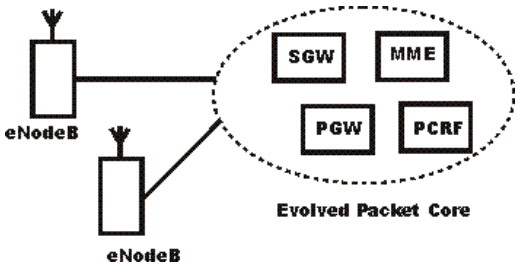


Рис. 2.2 Архітектура ядра мережі SAE.

SAE є еволюційним продовженням ядра мережі GPRS, з деякими відмінностями:

- спрощена архітектура - архітектура SAE знижує експлуатаційні та капітальні витрати. Нова плоска модель означає, що потрібно підвищити пропускну здатність вузлів тільки двох типів (базових станцій і шлюзів), щоб вони впоралися з трафіком в разі його значного зростання.
- цілком побудована на IP (AIPN) – перші концепції 3G було розроблено для того, щоб голос, як і раніше передавався по системі з комутацією каналів. З тих пір спостерігався перехід до IP-мереж. Відповідно архітектура SAE побудована на базі IP-мережі.
- забезпечує більшу пропускну здатність мережі радіодоступу (RAN) – передбачається, що низхідний канал (Down Link) буде мати швидкість понад 100 Мбіт/с, і основна увага системи буде зосереджена на мобільності смуги пропускання, мережа повинна буде підтримувати набагато більше рівнів даних.
- забезпечує меншу затримку RAN - зі збільшенням необхідних рівнів взаємодії і більш швидких відповідей, SAE концепція забезпечить рівень затримки в районі 10 мс.
- підтримує мобільність між декількома гетерогенними RAN, що включає підтримку, як систем типу GPRS, так і не-3GPP систем (наприклад WiMAX). [1]

Основним компонентом архітектури SAE є Evolved Packet Core (EPC). EPC служить еквівалентом мережі GPRS. Архітектура EPC показана на Рис. 2.3.

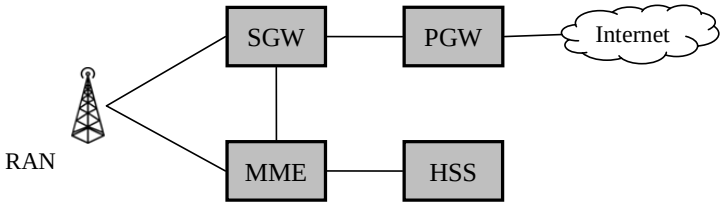


Рис. 2.3 Типова архітектура EPC/LTE

Архітектура EPC є мережею All-IP з комутацією пакетів, який вміщує різні схеми бездротового доступу, такі як Long Term Evolution (LTE). Мережа EPC складається з різних вузлів: Evolved NodeB (eNB) вузла для радіодоступу LTE, об'єкта керування мобільністю (MME) – вузол для керування мобільності терміналу, вузла домашньої абонентської системи (HSS), вузла бази даних інформації про користувачів, вузла облслуговуючого шлюза (SGW), вузла якірної точки мобільності для керування терміналами, а також вузла шлюза пакетної мережі передачі даних (PGW), який служить шлюзом між терміналами і зовнішніми мережами, такими як Інтернет. [2]

MME – це ключовий контролюючий модуль для мережі доступу LTE. Він відповідає за процедури забезпечення мобільності, хендовера, стеження і пейджінга UE. Він бере участь в процесах активації/дезактивації мережевих ресурсів і так само відповідає за вибір SGW для UE при початковому підключенні і при хендовері всередині LTE зі зміною вузла ядра мережі (CN). Він відповідає за аутентифікацію користувача (при взаємодії з HSS).

SGW – призначений для обробки і маршрутизації пакетних даних, що надходять в підсистему базових станцій. SGW маршрутизує і направляє пакети з одними даними, в той же час виконуючи роль вузла керування мобільністю для даних користувача при хендовері між базовими станціями (eNodeB), а також вузла керування мобільністю між мережею LTE і мережами з іншими технологіями 3GPP. Коли UE вільний і не зайнятий викликом, SGW відключає низхідний канал даних (DL) і створює пейджинг, якщо потрібно передати дані по DL в UE напрямку. Він керує і зберігає стани UE (наприклад вимоги до пропускної здатності для IP-сервісів, внутрішню

інформацію мережевої маршрутизації). Він також надає копію даних користувача при узаконеному перехопленні.

PGW – забезпечує з'єднання від UE до зовнішніх пакетних мереж даних, будучи точкою входу і виходу трафіку для UE. UE може мати одночасно з'єднання з більш ніж одним PGW для підключення до декількох мереж. PGW виконує функції захисту, фільтрації пакетів для кожного користувача, підтримку білінгу, узаконеного перехоплення і сортування пакетів. Інша важлива роль PGW - бути вузлом керування мобільністю між 3GPP і не-3GPP технологіями, такими як WiMAX і 3GPP2 (CDMA 1X і EVDO).

HSS – це центральна база даних, яка містить інформацію про користувача. Функції HSS включають мобільність, керування викликами і підтримкою встановлення сеансу, аутентифікацію і авторизацію користувачів. HSS базується на pre-Rel-4 Home Location Register (HLR) і центрі аутентифікації (AuC).

2.2. Протоколи гарантії якості в мережах доступу і на рівні ядра мережі

Протокол: NBAP (Node B Application Part).

Оркестрація та менеджмент (O&M) базової станції UMTS (Node B) Node B розділена на дві частини: O&M, пов'язана з фактичною реалізацією базової станції, позначена як конкретна реалізація (Implementation Specific) O&M, та O&M, що впливає на ресурси передачі трафіку в базовій станції, яка управляється контролером радіомережі, позначена як логічна O&M. Архітектура контролера мережі (RNC) з інтерфейсами O&M показана на Рис.2.4.

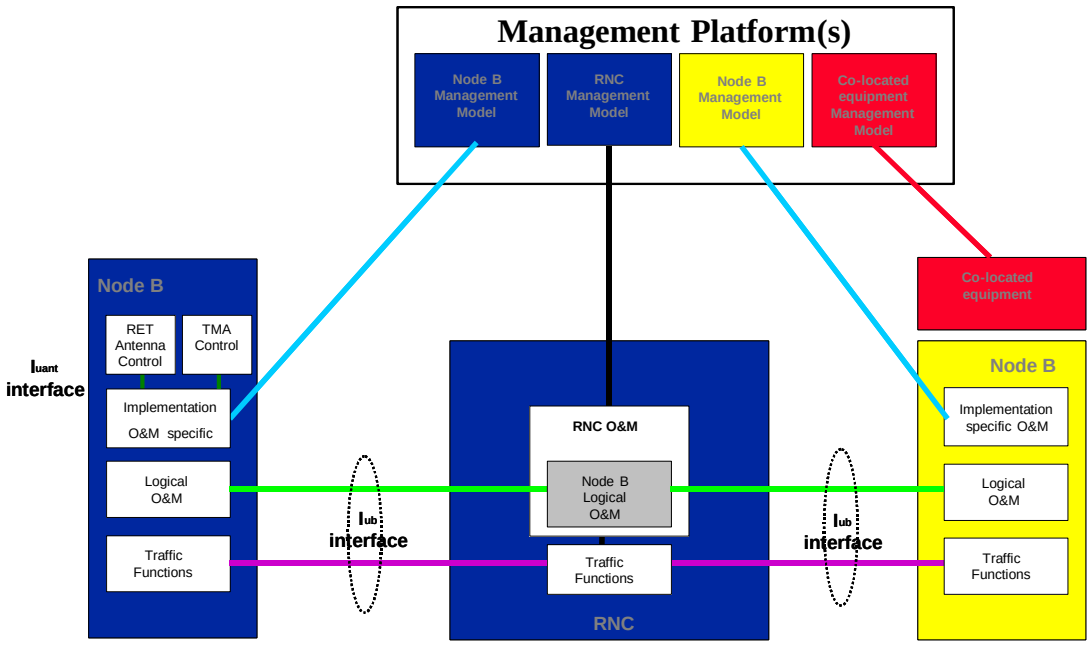


Рис. 2.4 Архітектура контролера мережі з інтерфейсами O&M

На функції конкретної реалізації O&M значною мірою впливає реалізація базової станції (NodeB), як з точки зору її апаратних компонентів, так і з точки зору управління компонентами програмного забезпечення. Тому функції є залежними від реалізації та виконуватися між базовою станцією та системою управління.

Як варіант транспортного рішення для конкретної реалізації O&M - це маршрут від базової станції до системи управління через контролер мережі RNC. У цьому випадку інтерфейс конкретної реалізації O&M для та інтерфейс Iub мають одного і того ж фізичного каналу, а TS 25.442 [4] визначає функцію маршрутизації та транспортного каналу для цього сценарію. Розгортання маршрутизації через RNC в UTRAN є необов'язковим. Там, де потрібна сигналізація між спільно розміщеним обладнанням та його системою управління, вона може бути перенесена на той самий канал, що і конкретна реалізація O&M.

Логічна O&M - сигналізація, пов'язана з контролем логічних ресурсів (каналів, сот, ...), що належать контролеру мережі RNC, але фізично реалізовані у базовій станції. Контролер радіомережі контролює ці логічні ресурси. Ряд процедур O&M, фізично реалізованих у Node B, впливають на логічні ресурси, і тому вимагають обміну інформацією між RNC та Node B. Усі повідомлення, необхідні для підтримки цього інформаційного обміну, класифікуються як логічні O&M, які є невід'ємною частиною сигнального протоколу NBAP (Node B Application Part).

QoS протоколи

Функція (TF, Translation Function) *трансляції* перетворює внутрішні примітиви послуг мережі LTE в модулі різних протоколів взаємодіючих зовнішніх мереж, включаючи перетворення атрибутів послуг мережі LTE в параметри QoS протоколів зовнішніх мереж.

Функція управління можливостями (A/CCF, Admission / Capability Control Function) забезпечує інформацією про усі можливі ресурси мережевих вузлів, визначаючи при кожному запиті (чи модифікуванні) послуги, чи можуть мережеві вузли забезпечити необхідні ресурси. Ця функція також контролює можливість надання самої послуги, тобто чи реалізована в мережі запитана послуга.

Функція керування підпискою (SCF, Subscription Control Function) забезпечує контроль доступності абонентам певних послуг з необхідними параметрами QoS.

Відповідно до рекомендації 3GPP TS 23.402 V15.1.0 (2017-09), модель QoS, яка застосовується в поєднанні з опорними точками на основі протоколу PMIP, не використовує ідентифікатори каналів у пакетах площини користувача. Вона базується на фільтрах пакетів та пов'язаних з ними параметрах QoS (QCI, ARP, MBR, GBR), що надаються системі доступу через позамаршрутну (off-path) сигналізацію.

PCRF сигналізує ті ж фільтри пакетів та пов'язані з ними параметри QoS через Gxa, Gxb та Gxc, що і через Gx; інакше кажучи, деталізація інформації QoS, яка передається через Gxa, Gxb та Gxc, така ж, як і через Gx.

Канал EPS з S5/S8 на основі протоколу PMIP і протоколу доступу E-UTRAN показано на Рис. 2.5.

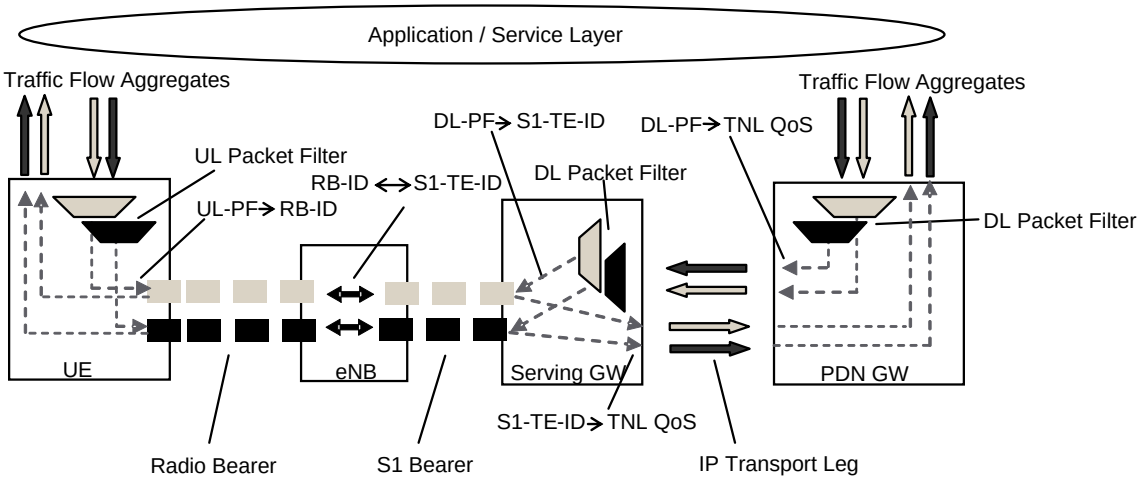


Рис. 2.5 Два канали Unicast EPS (S5/S8 на основі PMIP та протокол доступу E-UTRAN)

Для S5/S8 на основі протоколу PMIP та протоколу доступу E-UTRAN, канал EPS містить конкатенацію одного радіоканалу та одного каналу S1. Служба підключення PDN між обладнанням користувача (UE) і зовнішньою мережею пакетної передачі даних підтримується шляхом об'єднання каналу EPS та IP-з'єднання між шлюзом обслуговування і шлюзом PDN. Контроль QoS між Serving GW і PDN GW забезпечується на рівні транспортної мережі (TNL).

Канал EPS реалізується наступними елементами:

- В обладнанні користувача UFT TFT відображає агрегат потоку трафіка до каналу EPS у напрямку висхідної лінії зв'язку.

- У шлюзі обслуговування (Serving GW) DL TFT відображає агрегат потоку трафіку до каналу EPS у напрямку низхідної лінії зв'язку.

- радіоканал передає пакети каналу EPS між UE та eNodeB. Існує одноразове відображення між каналом EPS та радіоканалом.

- Канал S1 переносить пакети каналу EPS між eNodeB і шлюзом обслуговування. Існує одноразове відображення між каналом EPS та каналом S1.

- Для кожного обладнання користувача в туннелі PDN транспортуються пакети каналу EPS між шлюзом обслуговування та шлюзом PDN. Між каналом EPS та цим тунелем реалізується відображення «багато до одного».

- UE зберігає відображення між фільтром пакетної передачі висхідної лінії зв'язку та радіоканалом для створення зв'язків між агрегатом потоку трафіку та радіоканалом у висхідній лінії зв'язку.

- eNodeB зберігає відображення «один до одного» між радіоканалом та каналом S1, щоб створити зв'язок між радіоканалом та каналом S1 як у напрямку висхідної лінії зв'язку, так і в напрямку низхідної лінії зв'язку.

- Шлюз обслуговування зберігає відображення «один до одного» між фільтром пакетної передачі по низхідній лінії зв'язку та каналом S1, щоб створити відображення між агрегатом потоку трафіку та каналом S1 у низхідній лінії зв'язку.

- Шлюз доступу до інших мереж (PDN SW) забезпечує APN-AMBR для всіх SDF тих самих APN, які пов'язані з QCI без GBR.

Параметри QoS мають першочергове значення для технології SDN. При цьому важливо враховувати зв’язок між типом прикладних програм (передача даних в реальному часі чи передача файлів) та параметрами мережі, такими як доступна смуга пропускання, втрати пакетів, затримки або джиттер. –

В таблиці наведено вимоги до параметрів якості обслуговування SDN для різного типу трафіку.

Таблиця 2.1

Вимоги до параметрів якості обслуговування SDN

Тип трафіку	**Затримка**	**Втрати пакетів**	**Джиттер**	**Смуга пропускання**
Голосова телефонія (VoIP)	≤ 150 мс	≤ 1%	< 30 мс	21-320 кбіт/с
Інтерактивне відео	≤ 150 мс	≤ 1%	≤ 30 мс	–
Потокове відео	≤ 4-5 мс	≤ 1%	–	–

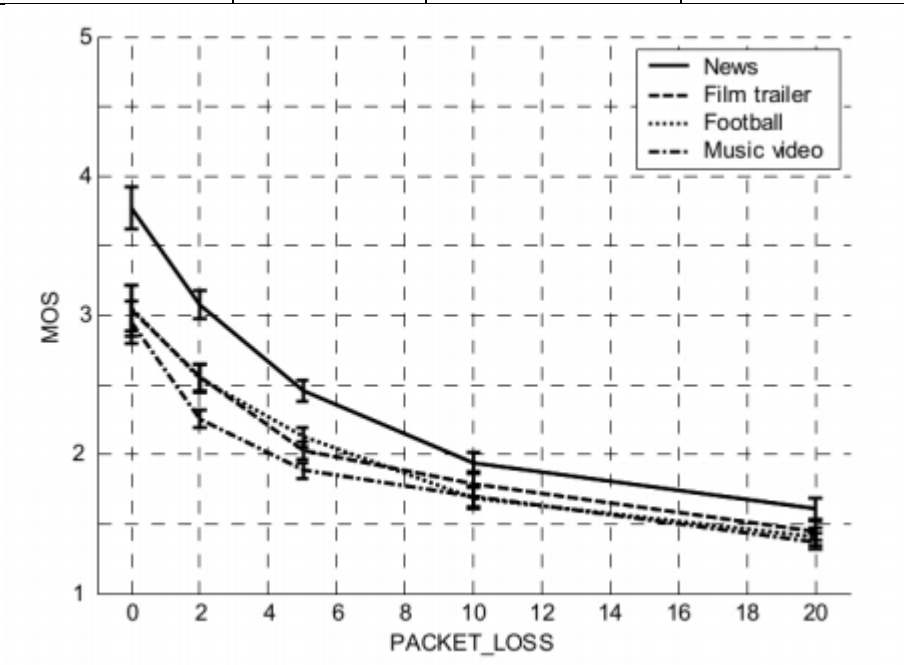


Рис. 2.6 Графік втрати пакету

Голосова телефонія не терпить втрат пакетів (в ідеалі, їх взагалі не повинно бути), особливо якщо використовується стиснутий кодек.

Максимальна затримка потокового відео залежить від буферизації відео-додатків, тому вона може бути меншою за вказане значення.

Допустиме значення джиттера не є основним параметром для прикладних програм, що використовують потокове відео, тому для нього немає визначених вимог.

Вимоги до пропускної здатності потокового відео пов’язані з форматом кодування і швидкістю відеопотоку, тому вони не мають фіксованого значення.

Висновки:

У другому розділі було проаналізовано та описано механізм LTE, також проведено ознайомлення з перевагами та недоліками LTE. При аналізі вже відомих механізмів також пройшло ознайомлення з архітектурою мережі SAE, EPC/LTE. Були досліджені наступні протоколи гарантії якості в мережах доступу: NBAP (Node B Application Part), QoS протоколи. Ми підходимо до висновку про те що поточні мережі 4G не витримують вимог, висунутих новими сценаріями застосування на данний час, тому технологія 5G на разі дуже актуальна.

РОЗДІЛ 3.

ГАРАНТУВАННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ

3.1. Процедура гарантування заданої якості обслуговування

Принцип динамічного контролю якості полягає у наступному: значення затримки у обслуговуванні заявки на встановлення з'єднання (роз'єднання, відновлення) порівнюється із політикою якості обслуговування відповідного абонента. Якщо показник не відповідає, тоді послідовно порівнюються показники якості у віртуальних вузлах та каналах зв'язку віртуальної мережі із пороговими значенням відповідних політик збережених у підсистемі PCRF. Даний принцип аналізує такі кількісні показники ефективної роботи системи, як: час затримки заявки службового потоку у віртуальному вузлі та ймовірність втрати запитів у вузлі обслуговування. Вузол обслуговування - це віртуальна машина яка виконує функції керування мережевого вузла.

Після того, як було виявлено де саме є проблема зниження показників ефективності обслуговування приймаються міри: Якщо проблема у часі передачі між вузлами обслуговування, то рекомендується зробити реконфігурацію системи, а саме змінити розміщення віртуальних вузлів у фізичних вузлах гетерогенної структури датацентрів. Якщо проблема ідентифікована у одному вузлі обслуговування, тоді рекомендовано збільшити кількість ресурсів обслуговування. Якщо спостерігається зниження показників якості обслуговування у групі вузлів зв'язаних інтерфейсів, наприклад які утворюють єдине ядро мережі EPC, тоді рекомендовано обмежити потік заявок які направляються на обслуговування відповідного ядра. Для цього рекомендовано розрахувати інтенсивність навантаження на групу вузлів. Алгоритм процедури наведений на Рис. 3.1.

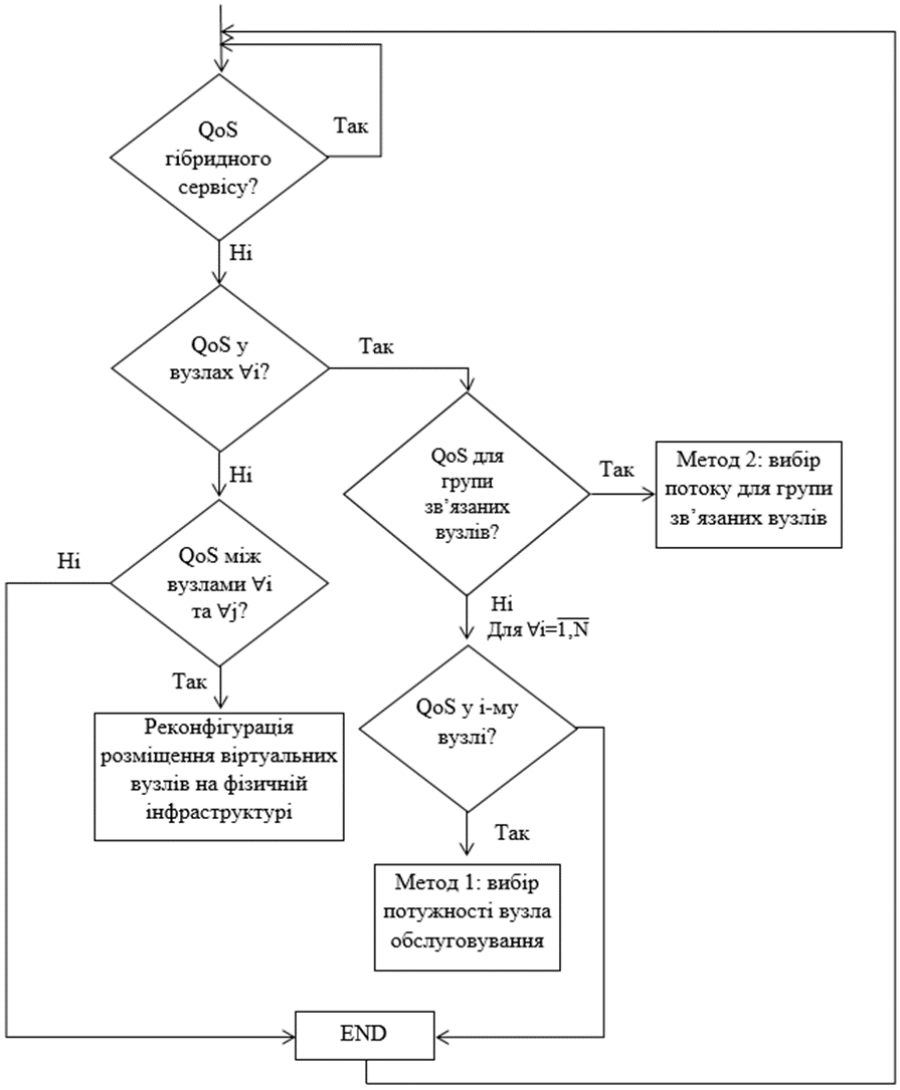


Рис. 3.1 Процедура гарантування заданої якості обслуговування.

Для реалізації принципу динамічного контролю якості потрібна модифікація підсистем системи PCRF. Підсистема «Єдине сховище політик» розширюється, додаються наступні політики відносно показників якості обслуговування потоків керування:

1. Допустимий час затримки заявки службового потоку у віртуальному вузлі.

2. Допустимі втрати запитів у віртуальному вузлі

3. Допустимий час обслуговування запитів у групах віртуальних вузлів які забезпечують заданий сервіс.

4. Допустимі затримки при передачі між вузлами обслуговування

5. Значення допустимих затримок доставки керівного впливу на мережеві вузли.

Розширена підсистема зображена на Рис. 1.2.

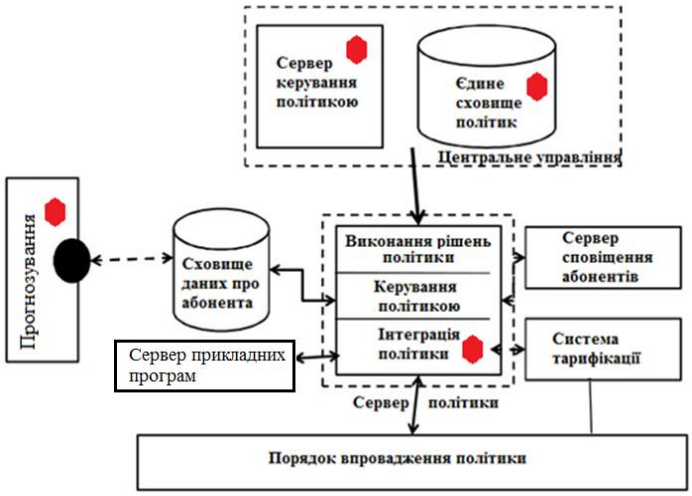


Рис. 1.2 Модифікація підсистеми PCRF.

• Підсистема «Керування політикою» формує групу вимог до виконання набору політик по відношенню до різних потоків керування.

• Підсистема «Сервер політики» виявляє проблему невідповідності поточних показників якості заявленим політикам обслуговування відповідного абонента.

• У підсистемі «Сервер прикладних програм» реалізовані програмні модулі в яких виконуються обчислення відповідно до запропонованих методів. Вихідним даними для методів є статистичні дані отримані від системи моніторингу та дані про політики, які забезпечуються для відповідних абонентів.

• Підсистема «Сховище даних про абонента» доповнюється інформацією про віртуальні вузли, або створюється окрема база даних інформації про статистику функціонування віртуальної мережі обслуговування, де збирається інформація про потоки заявок на обслуговування, статистика відносної залежності інтенсивності обслуговування від ресурсів обслуговування диференційовано для кожного типу запитів.

Принцип динамічного контролю якості обслуговування потребує нових процедур: необхідно організувати взаємодію системи керування мобільного зв’язку із системою керування віртуалізованими ресурсами (Рис. 3.3).

Контроль якості виконання керівних процедур оцінюється на рівні абонентського пристрою:

Абонентський пристрій фіксує час затримки у виконанні службових процедур, а саме час від моменту ініціалізації з’єднання до моменту початку передачі даних, та передає підсистемі PCRF.

PCRF отримує цю інформацію від абонента та аналізує на сервері політик; у підсистемі виконання рішень політики порівнює отримані дані на відповідність обраної політики, яка відповідає абоненту та зберігається у «Сховищі даних про абонента».

Якщо значення параметрів затримок не відповідають політиці, PCRF робить запит до підсистеми «Оркестратор» для визначення групи вузлів *i*, які обслуговують відповідного абонента.

Підсистема «Оркестратор» надсилає номери вузлів, які обслуговують абонента, розташованого у заданій місцевості. PCRF відправляє підсистемі «Моніторинг хмарних прикладних програм» запит для отримання інформації про час затримки та показники втрат у вузлах *i*, а також інформацію про затримки між вузлами обслуговування. Система моніторингу хмарних прикладних програм збирає інформацію відносно показників затримки та втрат гібридних сервісів, які обслуговуються у вузлах віртуальної мережі. Дані відносно групи вузлів обслуговування і передають у PCRF, де реалізовано принцип динамічного контролю якості обслуговування гібридних сервісів. Відповідно до керівних рішень, підсистема PCRF направляє запити:

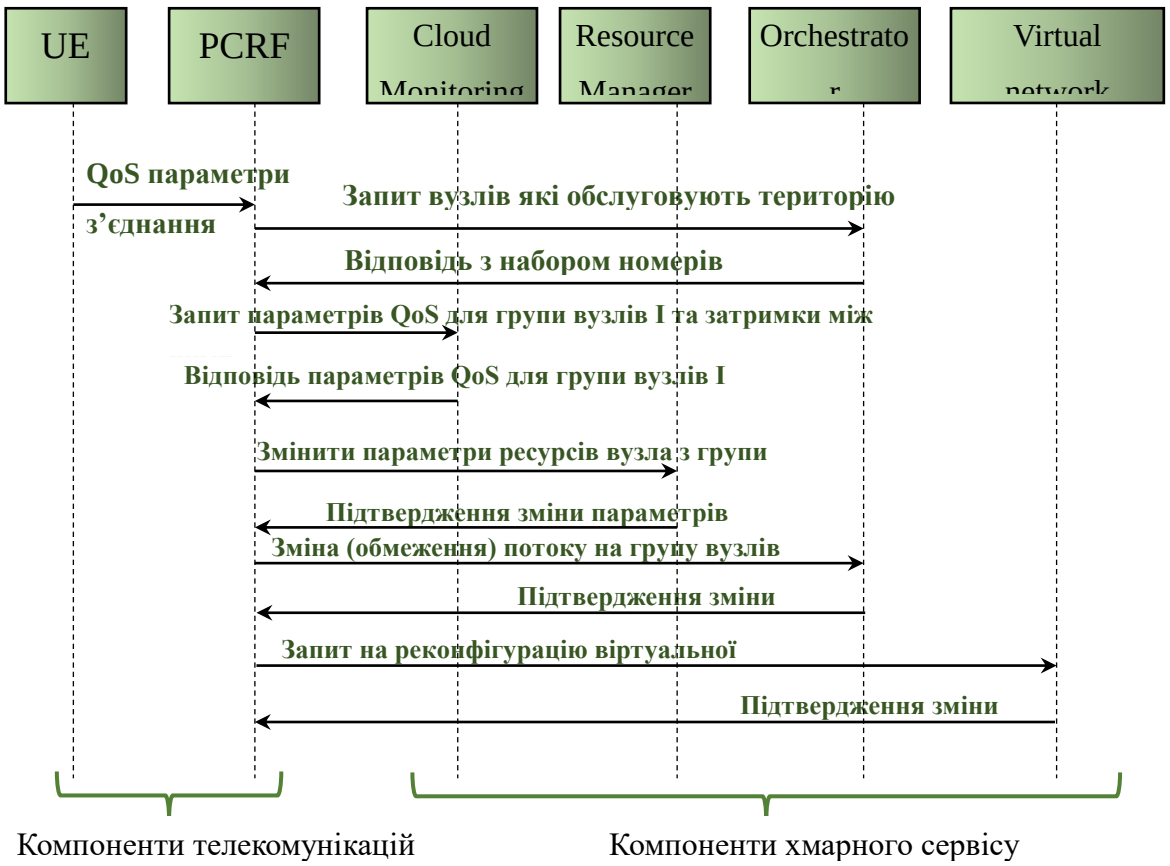


Рис. 3.3 Взаємодія системи керування мобільного зв'язку та системи керування віртуалізованим середовищем.

- на реконфігурацію віртуальної мережі, до «Менеджера віртуальної мережі»;

- на реконфігурацію ресурсів до «Менеджера ресурсів»;

- на зміну потоків обслуговування до «Оркестратора» потоків по віртуальній мережі.

При реалізації принципу динамічного контролю якості обслуговування задіяно більшість підсистем системи PCRF.

3.2. Інтеграція SDN в мобільних мережах

Є кілька робіт, які описують інтеграцію SDN в мобільних мережах [5-9]. Вони пропонують додавати SDN-агенти в елементи мобільної мережі. SoftRAN [5] пропонує централізовану архітектуру в якості альтернативи розподіленому рівню керування, який реалізується в даний час в LTE

мережах. Це абстрагує всі базові станції, розгорнуті в географічній зоні в якості великої віртуальної базової станції. Всі фізичні базові станції виглядають як радіоелементи з мінімальною логікою керування. Ці радіо елементи потім керуються централізованим елементом. CellSDN [6] надає детальну класифікацію пакетів комутаторам доступу, яка може бути реалізована в програмному забезпеченні (наприклад, з використанням відкритого VSWITCH). Інші роботи [7-9] визначають, що кожна базова станція має комутатор доступу, який виконує детальну класифікацію пакетів на шляху від мобільного терміналу. Комутатори доступу можуть бути програмними (наприклад, Open vSwitch). Сервер також може мати локального агента, який кешує політики обслуговування для мобільних терміналів, щоб звести до мінімуму взаємодію з центральним контролером.

Інша частина ядра мережі складається з комутаторів, в тому числі кількох шлюзів, підключених до Інтернету. Ці основні комутатори виконують багатовимірну класифікацію пакетів на високій швидкості для кількох тисяч або десятків тисяч правил.

В даний час існують лише кілька поглиблених наукових доповідей, що стосуються мобільних мережевих архітектур, які поєднують в собі поняття хмарних обчислень, SDN та NFV. Перші архітектурні пропозиції - особливо в контексті хмарних-RAN - включають відображення мережевих функцій, необхідних для інтеграції мобільних мереж з технологією SDN. Це лише функції контролю мобільного зв'язку, тобто MME, HSS, PCRF і рівня керування S/P-GW. Додаткові функції включають в себе транспорт, балансування навантаження, безпеку, політики, білінг, моніторинг, QoE або оптимізацію ресурсів. Ці функції працюють в мобільній Cloud мережі як SDN-прикладні програмні компоненти. При такому підході, призначений для користувача рівень складається тільки із стратегічно розташованих SDN сумісних комутаторів і звичайних комутаторів. SDN комутатори замінять повністю або частково поточний транспорт мобільної мережі [10-11]. Це консолідована архітектура показана на Рис. 3.4.

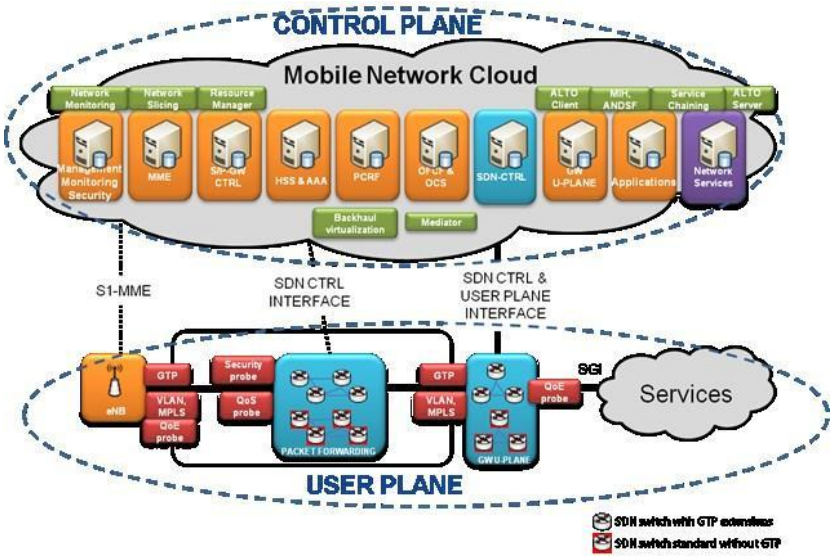


Рис. 3.4 Консолідована архітектура мобільної мережі

Необхідні елементи мережі EPC працюють в хмарі. Затримка може вплинути на розташування розгортання деяких обчислювальних вузлів, що працюють віртуально. Деякі стратегічні функції можуть бути розміщені близько до важливих вузлів, створюючи таким чином децентралізовану хмару.

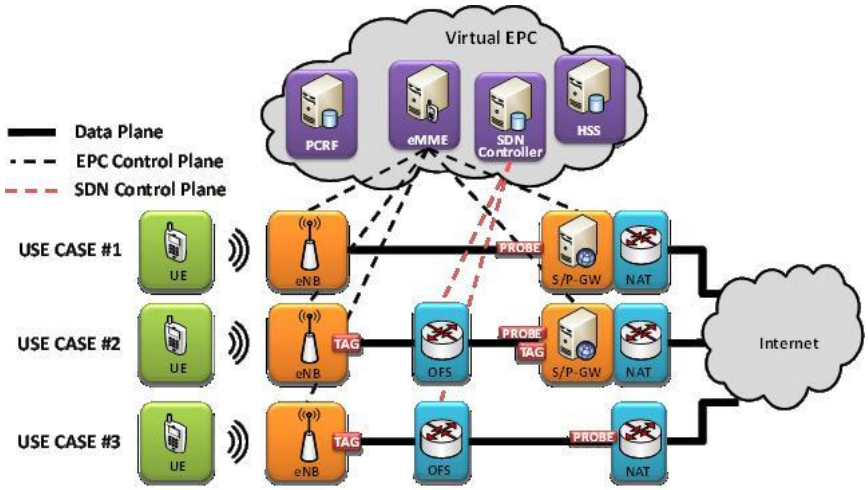


Рис. 3.5 Сценарій міграції з використанням OpenFlow.

Рис. 3.5 являє собою 3-крововий сценарій міграції з використанням OpenFlow як протоколу зв'язку з SDN. Перший випадок використання (тобто UC1) відповідає традиційній LTE архітектурі, зі старими вузлами. Другий випадок використання (тобто UC2) вводить технологію SDN для керування

2-м рівнем маршрутизації на ядрі мобільної мережі, зберігаючи старі вузли. Цей сценарій є гібридним підходом. І, нарешті, третій випадок використання (тобто UC3) зображує повністю сумісну мережу SDN.

Висновки:

В третьому розділі досліджувались процедури гарантування якості обслуговування, описувався принцип динамічного контролю. Було виявлено ряд проблем та описані методи їх подолання. Одна з них це: зниження показників ефективності обслуговування, яка вирішується одним з методів: 1) реконфігурацією системи 2) обмеженням потоку заявок які направляються на обслуговування відповідного ядра. Також в цьому розділі була описана інтеграція SDN в мобільних мережах.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

В ході дослідження були вивчені і описані основні поняття і принципи 5G мереж. Концепція мереж п'ятого покоління передбачає розгортання надщільних мереж з високошвидкісним доступом поверх вже існуючих мереж, які будуть забезпечувати загальне покриття. Проаналізувавши свою тему: << Аналіз процедур забезпечення якості у мобільних мережах 5G >> було проведено ознайомлення та опис наступних технологій та механізмів:

- Ознайомлення з технологією 5G
- SDN
- Опис сервісів які надаються
- Вимоги до якості
- Опис механізмів контроля LTE
- Протоколи гарантії якості в мережах доступу
- Процедура гарантування заданої якості обслуговування.

На підставі зробленого нами дослідження можна зробити наступні висновки: було виявлено недоліки та переваги SDN, 5G, LTE технологій, при їх більш детальному вивченню та огляду були знайдені рішення різних проблем даних механізмів та технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тихвинский В. О., Бочечка Г. С. Концептуальные аспекты создания 5G //Электросвязь. – 2013. – №. 10. – С. 29-33.
2. Оссейран А. Технологии мобильной связи 5G: анализ и перспективы //Первая миля. – 2013. – №. 38. – С. 16-21.
3. Тихвинский В. О., Бочечка Г. С. Перспективы сетей 5G и требования к качеству их обслуживания //Электросвязь. – 2014. – Т. 11. – С. 40-43.
4. Лапонина О. Р., Сухомлин В. А. Способы трансформации сетей к SDN-архитектуре //International journal of open information technologies. – 2015. – Т. 3. – №. 4.
5. Гузев О. Ю., Чижов И. В. Балансировка нагрузки в защищенных сетях с использованием технологии SDN //Системы и средства информатики. – 2018. – Т. 28. – №. 1. – С. 123-138.
6. Тихвинский В. О., Терентьев С. В., Высочин В. П. Сети мобильной связи LTE/LTE Advanced //М.: Медиа Паблишер. – 2014.
7. Гельгор А. Л. Технология LTE мобильной передачи данных: учебное пособие. – 2011.
8. Тихвинский В. О., Терентьев С. В., Юрчук А. Б. Сети мобильной связи LTE: технологии и архитектура //М.: эко-Трендз. – 2010. – Т. 284.
9. Гаркуша С. В., Василенко Ю. А. Модель планирования частотно-временного ресурса в нисходящем канале связи технологии LTE //Научно-технический вестник информационных технологий, механики и оптики. – 2013. – №. 3 (85).
10. Климаш М. М. и др. Покращення параметрів радіоінтерфейсу LTE/HSOPA //Комп'ютерні технології друкарства, Львів. – 2011. – №. 26. – С. 130-137.

11. Тихвинский В. О., Бочечка Г. С. Перспективы внедрения технологии узкополосной передачи данных NB-IoT в сетях LTE //Электросвязь. – 2016. – №. 8. – С. 10.
12. Липинский А. В. Оптимизация технологии передачи голоса в сетях LTE-VOLTE при хорошем качестве и низком уровне энергопотребления мобильными устройствами //Моделирование, оптимизация и информационные технологии. – 2016. – №. 1. – С. 9-9.
13. Одарченко Р. С. и др. Дослідження перспективних технологічних рішень для стільникових мереж сімейства стандартів 5G //Стандартизація. Сертифікація. Якість. – 2016. – №. 6. – С. 14-19.
14. Нікіфоренко А. К. и др. СТАН РОЗВИТКУ МЕРЕЖ 5G. – 2017.
15. Одарченко Р. С., Абакумова А. О., Дика Н. В. Дослідження вимог до стільникових мереж нового покоління та можливості їх розгортання в україні //Проблеми інформатизації та управління. – Т. 2. – №. 54. – С. 52-59.
16. Григоренко Д. К., Одарченко Р. С. ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖ П’ЯТОГО ПОКОЛІННЯ 5G //Тези доповідей V Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і техніці»(ІТОНТ-2020): Черкаси, 21-23 травня 2020 р.–Черкаси. – С. 66.
17. Скулиш М. А., Заставенко А. А. Метод контролю якості обробки інформаційних потоків у мережі 5G. – 2016.
18. Лунтовський А. О., Семенко А. І. Застосування технологій SDN для програмної реалізації провайдерського ядра систем мобільного зв’язку 5G майбутнього покоління //Зв'язок. – 2014. – №. 3. – С. 13-19.

19. Глоба Л. С., Марціленко С. В. ЗАСТОСУВАННЯ ПРОГАМНО-ВИЗНАЧУВАНИХ МЕРЕЖ (SDN) В ТЕХНОЛОГІЇ 5G //Збірник матеріалів Міжнародної науково-технічної конференції «ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ»(ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ). – 2016.
20. Гуськов П. О., Максимюк Т. А., Климаш М. М. Метод динамічного формування структури рівня радіодоступу для мереж 5G. – 2015.
21. Старкова О. В. Моделі та методи оптимізації TCP-сеансів у мультисервісних телекомунікаційних мережах. – 2010.
22. Бугиль Б. А. и др. Методи оптимізації фізичної та логічної структур телекомунікаційних мереж. – 2013.